Retos y oportunidades del

Entretenimiento en línea

Actas del VIII Congreso Internacional Internet, Derecho y Política
Universitat Oberta de Catalunya. Barcelona, 9-10 Julio, 2012

Challenges and Opportunities of

Online Entertainment

Proceedings of the 8th International Conference on Internet, Law & Politics
Universitat Oberta de Catalunya. Barcelona, 9-10 July, 2012

COORDINADORES

Agustí Cerrillo i Martínez, Miquel Peguera
Ismael Peña-López, María José Pifarré de Moner,
Mònica Vilasau Solana

UOC Universitat Oberta de Catalunya

HUYGENS EDITORIAL

Retos y oportunidades del entretenimiento en línea

Actas del VIII Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona, 9-10 de julio de 2012

Challenges and Opportunities of Online Entertainment

Proceedings of the 8th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya, Barcelona, 9-10 July, 2012

2012

UOC
Universitat Oberta de Catalunya
www.uoc.edu

HUYGENS
EDITORIAL

RETOS Y OPORTUNIDADES DEL ENTRETENIMIENTO EN LÍNEA

CHALLENGES AND OPPORTUNITIES OF ONLINE ENTERTAINMENT

La Costa, 44-46, át. 1ª
08023 Barcelona
www.huygens.es

ISBN: 978-84-695-4123-4
Impreso en España

COMUNICACIONES SOBRE COMERCIO ELECTRÓNICO Y JUEGO ONLINE

Presentación

Agustí Cerrillo-i-Martínez
Miquel Peguera
Ismael Peña-López
María José Pifarré de Moner
Mònica Vilasau Solana
Comité de dirección
VIII Congreso, Internet, Derecho y Política

Se recogen en este volumen las actas de la octava edición del Congreso Internacional Internet, Derecho y Política (IDP 2012), celebrado en Barcelona los días 9 y 10 de julio de 2012. Bajo el título genérico de «Retos y oportunidades del entretenimiento en línea», el congreso ha tenido como foco principal los aspectos legales y políticos del entretenimiento en las redes digitales. Una vez más, el congreso ha convocado a investigadores, académicos y expertos de todo el mundo para analizar y debatir aspectos centrales del presente y el futuro de la red.

La creciente expansión de Internet y la mejora de las comunicaciones de banda ancha, así como la llegada de las redes de nueva generación, están propiciando un gran desarrollo del entretenimiento en línea. La expansión de las redes sociales, las plataformas de intercambio de contenidos audiovisuales generados por los usuarios, el juego online, o las nuevas fórmulas de distribución de cine bajo demanda, son sólo algunas manifestaciones de este fenómeno.

El entretenimiento en línea plantea multiplicidad de cuestiones relevantes en el plano jurídico, así como en el de la participación política y ciudadana. Entre otros puntos, se suscitan complejas cuestiones de privacidad y protección de datos, incluido el llamado derecho al olvido, sobre equilibrio entre propiedad intelectual y derechos fundamentales, la neutralidad de la red, protección de menores, políticas y gobierno de la red, derecho de acceso a la información pública, o responsabilidad de los prestadores de servicios de intermediación. Por otra parte las nuevas tecnologías inciden de modo directo en el acceso a la información y en el consiguiente robustecimiento del discurso público y de la participación democrática, particularmente en sociedades en que los medios tradicionales de comunicación se hallan bajo control político.

Centrado en estas cuestiones, pero sin olvidar otros aspectos relevantes en los campos del derecho y la política que plantean desafíos acuciantes para el futuro de Internet, el Congreso IDP 2012 ha constituido un lugar de discusión, análisis, formulación de propuestas y planteamiento de líneas de acción.

Las ocho ediciones del congreso IDP lo han consolidado como lugar de encuentro anual de investigadores, académicos y profesionales interesados en las consecuencias del uso de las tecnologías de la información y la comunicación en los diferentes ámbitos del derecho

y en la política. Destacados académicos e investigadores internacionales han participado en calidad de ponentes invitados en las diversas ediciones del congreso, entre otros, Benjamin Barber, Lilian Edwards, Jane Ginsburg, James Grimmelmann, Greg Lastowka, Ronald Leenes, Fred von Lohmann, Helen Margetts, Chris Marsden, Eben Moglen, Evgeny Morozov, John Palfrey, Yves Poullet, Stephano Rodotà, Alain Strowel o Jonathan Zittrain.

En el presente libro de actas se publican las comunicaciones académicas, enviadas por investigadores nacionales e internacionales al Congreso IDP 2012 y que tras superar un riguroso proceso de selección mediante revisión por pares fueron aceptadas para su presentación en el congreso. El congreso contó además con diversos ponentes invitados que intervinieron en diversas conferencias y mesas redondas, tal como consta en el programa que se incluye a continuación de estas líneas.

El congreso IDP es impulsado y organizado por los Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya (UOC) en el marco del Internet Interdisciplinary Institute (IN3), instituto que reúne la actividad de investigación de UOC centrada principalmente en el estudio de los efectos de la tecnología en las personas, las organizaciones y la sociedad en general. En su organización y desarrollo de la edición de 2012 han colaborado la revista IDP, el Postgrado en Administración electrónica de la UOC y el Postgrado en Distribución Audiovisual, VoD y Nuevos Modelos de Negocio FILMIN-UOC y la asociación Derecho del Entretenimiento Asociación Española (DENAE). El congreso IDP 2012 ha contado con el apoyo económico del Ministerio de Economía y Competitividad (DER2011-15788-E) y con el patrocinio del Grupo Francis Lefevbre.

Toda la información sobre el congreso se halla disponible en el sitio web http://edcp.uoc.edu/symposia/idp2012/

PROGRAMA

LUNES 9 DE JULIO

08:30 Recepción y acreditaciones

09:00 Bienvenida

Agustí Cerrillo i Martínez, Director de los Estudios de Derecho y Ciencia Política. Universitat Oberta de Catalunya.

09:15 Copyserfs and the Stationers' Company 2.0: How and why copyright law is evolving away from the protection of authors and toward the protection of intermediaries

Greg Lastowka Professor of Law, Rutgers University, USA. Author of Virtual Justice (Yale University Press, 2010)

10:15 Copyright Limitations, Exceptions, and Copyright's Innovation Policy

Fred von Lohmann. Senior Copyright Counsel at Google

11:00 Pausa café

11:30 Comunicaciones sobre propiedad intelectual

Moderadora: Raquel Xalabarder. Catedrática de Propiedad Intelectual de la Universitat Oberta de Catalunya.

Comunicaciones:

- Copyright infringing content available online. Federica Casarosa, European University Institute, Department of Law, Florence (Italy).
- Emulation is the Most Sincere Form of Flattery: Retro Videogames, ROM Distribution and Copyright. Benjamin Farrand, Lecturer in Intellectual Property Law, The University of Strathclyde (UK).
- The Digital Cloud Recorder: Modern VCR or New Intermediary? Robin Kerremans, consultant with Deloitte in Diegem, Brussels (Belgium); Geert Somers, Lawyer, Partner at time.lex, (Brussels), Affiliated Researcher ICRI-KULeuven (Belgium).
- Collective Licensing of On Line Music and the Recent Initiatives in the EU. Enrico Bonadio, Lecturer in IP law – City University London (UK).
- Cloud-Based cyberlocker services for music: other incoming battles in the endless war between copyright and technology? Aura Bertoni, Research Fellow in Intellectual Property Law, Bocconi University (Italy); Maria Lillà Montagnani, Assistant Professor of Commercial Law, Bocconi University (Italy).

13:00 Lunch

14:30 Sesiones paralelas

14:30 SALA ÁGORA: Comunicaciones sobre entretenimiento online

Moderadora: Blanca Torrubia Chalmeta. Profesora Agregada de Derecho mercantil. Universitat Oberta de Catalunya.

Comunicaciones:

- Myths and truths of online gambling. Margaret Carran, Lecturer, City Law School, City University, London (UK).
- Las nuevas tecnologías y el blanqueo de capitales: second life, entretenimiento online y método delictivo. Covadonga Mallada Fernández, Doctora en Derecho, Universidad de Oviedo.
- Cambiar las reglas del (video)juego. Mecanismos de control contractual en plataformas de entretenimiento online. Antoni Rubí Puig, Profesor Lector de Derecho Civil de la Universitat Pompeu Fabra, Barcelona.
- ¿Cómo influirá la nueva directiva 2011/83/UE en el comercio electrónico? Zofia Bednarz, Licenciada en Derecho, Universidad de Varsovia (Polonia). Estudiante de posgrado, Universidad de Málaga.

15:30 SALA ÁGORA: Mesa redonda sobre la regulación del Juego Online

Moderador: Francisco Pérez Bes. Abogado. Compliance Officer de Ladbrokes. Vicepresidente de ENATIC

Ponentes:

- Albert Agustinoy Guilayn. Abogado. Socio de DLA Piper. Experto en Derecho y Nuevas Tecnologías
- Alberto Palomar Olmeda. Profesor asociado del Departamento de Derecho Público del Estado (Área de Derecho Administrativo). Universidad Carlos III de Madrid. Coordinador de la obra El Juego on line (Aranzadi, 2011)

15:00 SALA BETA: Comunicaciones sobre derechos fundamentales

Moderador: Miquel Peguera Poch, profesor agregado de los Estudios de Derecho y Ciencia Política (UOC).

Comunicaciones:

- Constitución 2.0 y Estado de e-Derecho: a propósito del proceso constituyente islandés. Pere Simón Castellano, Becario de investigación (BR) del área de Derecho Constitucional de la Universitat de Girona.
- Redefiniendo la isegoría: open data ciudadanos. Helena Nadal Sánchez, Doctoranda del Departamento de Derecho Público de la Universidad de Burgos; Javier de la Cueva González-Cotera, Abogado.
- Conservación de datos e ilícitos en materia de propiedad intelectual: una visión constitucional de la Directiva 2006/24. María Concepción Torres Díaz, Profesora de Derecho Constitucional, Universidad de Alicante.
- Balancing Intellectual Property Against Data Protection: A New Right's Wavering Weight. Gloria González Fuster, Researcher at Vrije Universiteit Brussel (VUB), Research Group on Law Science Technology & Society (LSTS) (Belgium).
- La «Ley Sinde»: una oportunidad perdida para la regulación del ocio online en España. Ercilia García Álvarez, Catedrática Facultad de Economía y Empresa Universidad Rovira i Virgili; Jordi López Sintas, Profesor Titular de Universidad

Facultad de Economía y Empresa Universidad Autónoma de Barcelona; Sheila Sánchez Bergara, Estudiante de Doctorado de la Universidad Rovira i Virgili.

16:45 Pausa café

17:00 Mesa redonda: Nuevos modelos de negocio en la distribución de contenidos online

Moderadora: Judith Clarés. Profesora de los Estudios de Información y Comunicación de la Universitat Oberta de Catalunya

Ponentes:

- Jaume Ripoll, Director Editorial y socio fundador de filmin
- Josep Monleón, Head of Content, WUAKI.TV
- Sydney Borjas Piloto, Gerente de Artes Escénicas. Grupo SGAE.Grupo SGAE
- Liliana Alexandra Tamayo, Editorial El Derecho

18:30 Fin del primer día

MARTES 10 DE JULIO

09:00 Recepción y acreditaciones

09:30 Entretenimiento en línea y protección de los consumidores

Pedro A. de Miguel Asensio. Catedrático de Derecho internacional privado de la Universidad Complutense de Madrid. Autor de la obra Derecho Privado de Internet

10:30 Pausa café

10:50 Comunicaciones sobre privacidad y comercio electrónico.

Modera: Mª Rosa Llácer Matacás. Catedrática de Derecho Civil. Universitat de Barcelona.

Comunicaciones:

- Handling cookies within the european union: making the cookies crumble? Eleni Kosta, Senior Research Fellow, Interdisciplinary Centre for Law and ICT (ICRI)-KU Leuven (Belgium).
- Nuevos retos de la regulación jurídica y deontológica de la publicidad en las redes sociales. Esther Martínez Pastor, Prof. Contratado Doctor. Universidad Rey Juan Carlos; Mercedes Muñoz Saldaña, Prof. Contratado Doctor. Universidad de Navarra.
- El reto de la protección de datos de las personas mayores en la sociedad del ocio digital. Isidro Gómez-Juárez Sidera, Doctorando, Facultad de Administración y Dirección de Empresas, Universitat Politècnica de València; María de Miguel Molina, Profesora Titular, Departamento de Organización de Empresas, Universitat Politècnica de València
- PNR and SWIFT Agreements. External Relations of the EU on Data Protection Matters. Cristina Blasi Casagran, Researcher, Law Department, European University Institute, Florence (Italy).

- Online Entertainment in Cloud Computing Surroundings. Philipp E. Fischer, IT Lawyer. Sui Generis Consulting (CEO), Munich (Germany); Rafael Ferraz Vazquez, Media & Entertainment Lawyer. Veirano Advogados, Rio de Janeiro (Brazil).

13:00 Lunch

14:30 Comunicaciones sobre Derecho al Olvido

Moderadora: Mònica Vilasau Solana, profesora de los Estudios de Derecho y Ciencia Política (UOC).

Comunicaciones:

- The Emerging Right To Be Forgotten In Data Protection Law: Some Conceptual And Legal Problems. David Lindsay, Associate Professor, Faculty of Law, Monash University, Melbourne (Australia).
- El poder de autodeterminación de los datos personales en Internet. María Dolores Palacios González, Profesora Titular de Derecho civil, Universidad de Oviedo.
- Naming and Shaming in Greece: Social Control, Law Enforcement and the Collateral Damages of Privacy and Dignity. Lilian Mitrou, Associate Professor, Department Information and Communication Systems Engineering, University of the Aegean (Greece).

15:30 Comunicaciones sobre gobierno y políticas regulatorias

Moderador: Agustí Cerrillo i Martínez, profesor agregado y director de los Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya (UOC).

Comunicaciones:

- Guiding Principles for Online Copyright Enforcement. Andrew McDiarmid, Senior Policy Analyst, Center for Democracy & Technology, Washington, DC (USA); David Sohn, General Counsel, Center for Democracy & Technology (USA).
- Internet Co-Regulation and Constitutionalism. Christopher T. Marsden, Director of the Essex Centre for Comparative and European Law. Senior Lecturer, Essex School of Law (UK).
- Democracia electrónica, Internet y Gobernanza. Una concreción. Fernando Galindo Ayuda, Catedrático de Filosofía del Derecho, Universidad de Zaragoza.
- PIPA, SOPA, OPEN – The end of piracy or privacy? László Németh, PhD Student, Institute of Comparative Law, Faculty of Law, University of Szeged (Hungary).
- Reviving privacy: the opportunity of cyber-security. Maria Grazia Porcedda, Research assistant, Department of Law, European University Institute, Florence (Italy).

16:45 Pausa café

17:00 Mesa redonda: Privacidad en la red (mesa patrocinada por Google)

Ponentes:

- María González. Directora del Departamento Legal de Google para España, Portugal y Grecia.

- Esther Mitjans. Profesora Titular de Derecho Constitucional Universidad de Barcelona. Directora de la Autoridad Catalana de Protección de Datos.
- José Luis Piñar Mañas. Catedrático de Derecho Administrativo, Vicerrector de Relaciones Internacionales de la Universidad CEU-San Pablo (Madrid). Ex director de la Agencia Española de Protección de Datos.

Debate

18:30 Conclusiones.

Relator: Nacho Alamillo. Abogado. Director de Astrea

19:00 Fin del Congreso.

COMUNICACIONES SOBRE PROPIEDAD INTELECTUAL

CLOUD-BASED LOCKER SERVICES FOR MUSIC: OTHER INCOMING BATTLES IN THE ENDLESS WAR BETWEEN COPYRIGHT AND TECHNOLOGY?

Aura Bertoni*
Department of Legal Studies, Bocconi University, Research Fellow in Intellectual Property Law
Maria Lillà Montagnani*
Department of Legal Studies, Bocconi University, Assistant Professor of Commercial Law

ABSTRACT: Online distribution of digital content is likely to have entered a new phase characterized by cloud computing and whose business models are progressively altering at least as to music distribution. This change affects not only the business dimension of online distribution, but also the legal one by raising new questions as to the relationship between copyright law and technology. Indeed, as a new way of delivering technology, cloud computing is going to be at the heart of both legal and illegal distribution of digital content in the next future.

Hence, this work explores the innovative dimension of cloud-based locker services as adopted by music sites in order to identify, on the one hand, the similarities with former models of distribution and, on the other, the peculiar features inherent to models arising from cloud computing. It illustrates how cloud-based models represent the evolution of the traditional download- and stream-based distribution, as well as of the underlying revenue models by merging ad-based, subscription and pay-per-download systems.

In order to address the original elements in this renewed relationship between copyright and technology, we review the prior business models adopted for the online distribution of digital content so as to understand the way cloud computing provides a new model of distribution, and so, to start detecting the likely features of its emerging business models. This investigation is carried out with a specific focus on music distribution, which is now the market where services based on cloud computing are pervasively expanding.

KEYWORDS: Cloud computing, online distribution of music, copyright, cyberlockers, business models for online distribution of digital content.

1. INTRODUCTION

Online distribution of digital content is likely to have entered a new phase characterized by cloud computing and whose business models are progressively altering at least as to music distribution. This change affects not only the business dimension of online distribution, but

* Although this paper is born from a common elaboration, Section 2 is attributed to Maria Lillà Montagnani and Section 3 to Aura Bertoni, while the Introduction and Section 4 have been written jointly.

also the legal one by raising new questions as to the relationship between copyright law and technology. Indeed, as a new way of delivering technology, cloud computing is going to be at the heart of both legal and illegal distribution of digital content in the next future.

Hence, this work explores the specific dimension of cloud-based locker services as adopted by music sites in order to identify, on the one hand, the similarities with former models of distribution and, on the other, the peculiar features inherent to models arising from cloud computing. It illustrates how cloud-based models represent the evolution of the traditional download- and stream-based distribution, as well as of the underlying revenue models by merging ad-based, subscription and pay-per-download systems.

In order to address the original elements in the relationship between copyright and technology, the work is organized as follows. In section 2 we review the business models adopted for the online distribution of digital content, highlighting how legal and illegal distribution are intertwined. In section 3 we describe the phenomenon of cloud computing and the way it provides a new model of distribution for music. The reason for this choice lies in the fact that music is the market where services based on cloud computing are pervasively expanding. Finally, in section 4, we draw some initial remarks from this preliminary analysis about cloud-based locker services for music distribution concluding that they embody a cutting-edge topic, which is likely to gain a leading role in the future discourse on copyright law and online music distribution.

2. MODELS FOR ONLINE DISTRIBUTION OF DIGITAL CONTENT

The approach embraced to survey the models for online distribution of digital content is a chronological one, which also reflects the changes in the technology implemented. Accordingly, we start with the analysis of Digital Media Shops (DMSs) – that offered content for downloading in a way that mirrors the dynamics of offline distribution – and of, in parallel, peer-to peer (P2P) systems – which offered content for downloads, initially from a centralized server and afterwards via decentralized networks. This explains how the raising of DMSs and the spreading of P2P are intertwined. We follow by considering the streaming-based models that arose in connection with the spread of advertising as a revenue source, including the now established phenomenon of user-generated content (UGC).

2.1. The first models for online distribution of digital content: the rise of downloading

The DMSs have been the model for online distribution envisaged at legislative level in the WIPO Treaties in 1996 *(Copyright Treaty* (WCT) and *Performers and Phonograms Treaty* (WPPT))[1], subsequently implemented in the US through the *Digital Millennium Copyright*

1 *See* Mihaly Ficsor, The Law of Copyright and the Internet (Oxford University Press, 2002) (providing a thorough depiction of the negotiations that led to the WIPO Treaties and their provisions).

Act in 1998 (DMCA)[2], and in the EU through *the Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society*[3].

DMSs have been fully analysed in literature as the business model incentivised by law[4], the so called «digital copyright» entailing all treaties and acts before mentioned, which pushed for the adoption of digital rights management systems (DRMs) to enhance the control on content distributed online. These technologies, as well as the distribution model that they enable, were foreseen as the solution to the lack of control over the uses of copyright works that right holders complained as a consequence of the spread of digital technology and the Internet. In addition, they were also considered the tool to extend online the distribution models already implemented offline.

As a matter of fact, the choice for DMS-based distribution was triggered by the fear that the illegal distribution initiated by Napster (and its look-alikes) could establish in the digital environment: it should not surprise that the adoption of the DMCA preceded of just a couple of years the final decision on the Napster saga[5].

The well-known mechanism that Napster developed and offered was a centralized one. It relied on the downloading of specific software and the uploading of an index of files available for shared use to Napster's server. The files, however, remained stored on the hard

---

2 Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998) (hereinafter DMCA).

3 European Parliament and Council Directive 2001/29, 2001 O.J. (L 167) 10–19 (hereinafter Directive).

4 The analysis of business model for online distribution started in 2003 at the Berkman center – Harvard School of Law, within the Digital Media Project. See Gasser, Slater, Smith, Palfrey, Locke, McGuire, *Copyright and Digital Media in a Post-Napster World*, 2003, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2003-05.pdf; Id., *Copyright and Digital Media in a Post-Napster World*, Version 2 (version updated at January 2005), http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/wp2005.pdf; Gasser, McGuire, *Copyright and Digital Media in a Post-Napster World: International Supplement*, January 2005, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/wpsupplement2005_0.pdf; Gasser, Slater, Smith, Palfrey, Locke, McGuire, *Five Scenarios for Digital Media in a Post-Napster World*, 2003, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2003-07.pdf; Gasser et al., *iTunes How Copyright, Contract, and Technology Shape the Business of Digital Media. A Case Study*, 2004, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/GreenPaperiTunes041004.pdf; Slater, Smith, Bambauer, Gasser, Palfrey, *Content and Control: Assessing the Impact of Policy Choices on Potential Online Business Models in the Music and Film Industries*, 2005, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/content_control.pdf; Gasser, Ruiz Begue, *iTunes: Some Observations After 500 Million Downloaded Songs*, June 2005, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/iTunes_August_update_final[1].pdf; McGuire, Slater, *Consumer Taste Sharing Is Driving the Online Music Business and Democratizing Culture*, 2005, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/11-ConsumerTasteSharing.pdf.

5 Both the trial court and the court of appeals sanctioned Napster and accepted the plaintiff's claims in A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 911 (N.D. Cal. 2000); aff'd in part, rev'd in part 239 F.3d 1004, 1015 (9th Cir. 2001).

drives of the individual users' computers, and Napster's website only stored the index so facilitating the transfer from one user's computer to another's one. In essence, when a user connected to the Internet and requested a file from Napster's indexing system, the file was downloaded directly from the hard-drive of origin to that of the person requesting it. A centralized system, very similar to that of Napster, was adopted by Aimster[6]. Aimster, however, differed from Napster: apart from having adopted the necessary disclaimer as to the nature of the shared files, it also declared that it was not aware of the content exchanged because content was encrypted[7]. However, Aimster was sanctioned as, despite the fact that Aimster could not read the content of files exchanged, it was deemed not possible to affirm the complete ignorance of the fact that its software was used to violate copyright law.

Whereas DMSs were working out their success by enlarging their range of services from à-la-carte downloads to subscription and music «to rent», P2P technology was not surely slowed down by the Napster and Aimster decisions. While DMSs were opting for a proprietary management of copyright, i.e. an «all rights reserved» regime and the adoption of technical measures of protection, P2P networks continued to develop and be perfected, thereby becoming increasingly more difficult to target for the completely decentralized nature that they opted achieved.

In decentralized systems, each connected computer acts as a server, forming a super-hub[8], and a centralized indexing system is not necessary anymore. For this reason, in the *KaZaa* case[9], the producer of the software that was used to share files on Grokster's and Morpheus's networks, was initially absolved from the copyright infringement challenge, as it did not have any knowledge of the infringing nature of the shared content since encryption techniques were implemented. However, the U.S. Supreme Court subsequently overturned the decision on the grounds that the software was produced and distributed with the specific aim of monetary gain from the violations of copyright law that the users committed. The evidence that this was the case came from, first, the dissemination of advertising and promotional messages to attract downloaders of the P2P software; second, the absence of filters to identify infringing content, and, lastly, the possibility of receiving income from the sale of advertising on the website and from the transmission of promotional messages to users[10].

---

6 In re Aimster Copyright Litig., 334 F.3d 643, 650 (7th Cir. 2003).

7 *See* Jeffrey R. Armstrong, Sony*,* Napster*, and* Aimster*: An Analysis of Dissimilar Application of the Copyright Law to Similar Technologies*, 13 DePaul-LCA J. Art & Ent. L. & Pol'y 1, 7-12 (2003) (discussing the differences, from the technological point of view, between the software adopted by Aimster and Napster).

8 *See* Bryan H. Choi, *The* Grokster *Dead-End*, 19 Harv. J. L. & Tech. 393, 397 (2005-06) (discussing the differences between centralized and decentralized systems).

9 Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029 (C.D. Cal. 2003), *aff'd,* 380 F.3d 1154 (9th Cir. 2004), *rev'd*, 545 U.S. 913 (2005).

10 *See* Diane L. Zimmerman, *Daddy, Are We There Yet? Lost in* Grokster*-land*, Public Law & Legal Theory Research Paper Series, Working Paper No. 05-21, 2005, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=826064.

This was the first time that ad-based distribution was taken into consideration. Although, initially, it emerged as a revenue system implemented within P2P networks –as the analysis of the Grokster's business model shows– from there on it further expanded to become the most spread revenue model in the market of online distribution.

The above demonstrates how the model pushed by digital copyright was quickly overcome by market dynamics, which not only developed along the line of illegal models for distribution (the decentralized P2P networks), but also resulted in the adoption of P2P features for the legal distribution of digital content. Although there are few examples in concrete, «super-distribution»[11] and «P2P shops» constitute one of the first alternatives to DMSs that have been fully analysed in literature[12], as tools for enriching the online distribution models as well as for exploiting peer-to-peer networks for the legitimate exchange of authorised content. The idea behind this is that within the same networks that permit the sharing of digital content in violation of copyright, encrypted content can be introduced and shared on the conditions established by the right holder. The incentive provided for P2P users to exchange authorised content differs depending on the «P2P store» chosen, but it is generally a form of recompense (either monetary or often in the form of a point-collection system) whereby credit is earned whenever authorised –rather than infringing– files are shared.

One of the first examples of «super distribution» was initially developed to permit the embedding of encrypted files in the KaZaA and Grokster networks[13]. These files were identified by an Altnet icon which certified the legal circulation of content, allowing use of these files on payment of a sum determined by the content holder[14]. In substance, Altnet

11 The term «superdistribution» applied to creative works means a phenomenon of «multi-tiered distribution that starts with the owner of the content and enables entities at each step to redistribute content under their own business terms.» Bill Rosenblatt, *Learning from P2P: Evolution of Business Models for Online Content*, INDICARE (Dec. 10, 2004), http://www.indicare.org/tiki-read_article.php?articleId=61. *See also*, for the concept of superdistribution as applied outside copyright law,

12 Mori, Kawahara, *Superdistribution. The Concept and the Architecture*, in 73 The Transactions Of The Ieice 1133–1146 (1990), *available at* http://www.virtualschool.edu/mon/ElectronicProperty/MoriSuperdist.html.
Derek Slater, Meg Smith, Derek Bambauer, Urs Gasser, John Palfrey, *Content and Control*, *supra* note 4, at 16.

13 The circulation of Altnet files on Grokster network took place until the website was closed when the «United States Supreme Court unanimously confirmed that using this service to trade copyrighted material is illegal (…) [*and that t*]here are legal services for downloading music and movies. This service is not one of them» (http://www.grokster.com/). Instead, as far as KaZaA is concerned, it has been converted into an ad-supported distributor available only to US residents. *See* KaZaA homepage, http://www.kazaa.com/it/index.htm.

14 William W. Fisher, Urs Gasser, Derek Slater, Meg Smith & John Palfrey, *Comments on the OECD Working Party on Information Economy Draft Report «Digital Broadband Content: Music»*, Berkman Center for Internet & Society at Harvard Law School 6 (Jan. 10, 2005), *available at* http://cyber.law.harvard.edu/digitalmedia/oecd_comments.pdf.

incentivised the exchange of legal files on P2P networks (no longer in Grokster) at the price and according to the license methods decided by the content holder. Users who shared these files accumulated points that could then be used to claim prizes.

Another example of «super distribution» was Weed[15] which, at least initially, had a diffusion that was even more widespread than Altnet. Indeed, while Altnet circulated only on the KaZaA and Grokster networks, files from Weed could circulate freely in almost any file-sharing network. In this system, encrypted files could only be decrypted following payment, and could only be used under the conditions imposed by the content owner[16]. Generally, the file could be initially played a number of times without paying any fee. After this, payment was required to allow the file to be transferred to a limited number of players and from one to three computers. This represents the implementation of a system of pay-per-download within P2P networks. At the same time, it allowed a person to exchange files and become a distributor of purchased files based on a mechanism reminiscent of viral marketing by enabling the revenue sharing of the content between the author or music label, and the person who uploaded file into the P2P network. While the first right holder continued to receive a percentage of the sum paid for each download (whether carried out à-la-carte or within a file-sharing network), the uploader of the file to the Internet received their own percentage for up to three downloads. After that, the next purchaser who shared the file would receive earnings, together with the first right holder and Weed who always received a fixed percentage for each download carried out.

What is interesting is that on the wake of the «superdistribution» systems, also some DMSs (such as Napster, which morphed, after the Supreme Court's decision into a DMS) started to offer the sharing of acquired files with other subscribers of the same service alongside their traditional services[17], just as sites dedicated to «superdistribution» added services for downloads on payment of subscription[18].

Although a valuable attempt, the legal side of digital distribution was not enriched from a business model based on P2P networks. This might be related even to the fact that after a few cases Grokster-alike, the P2P networks evolved towards a third generation system that shows an higher degree of decentralization and no attempt was made to exploit them within legal models of distribution. In the BiTorrent architecture, which is most evolved P2P downloading system, files are not downloaded from a single source, but users join a

15 *The* Weedshare service has been suspended. See http://www.weedshare.com/.

16 Fisher *et al.*, *Comments on the OECD Working Party on Information Economy Draft Report*, *supra* note 14, at 6.

17 For example Napster launched «Napster Share», offered to registered users who were willing to upload their files in the legalized peer-to-peer network governed by Napster. The service is not open anymore.

18 Wippit (http://www.wippit.com/default.aspx) was one of the websites that added to the initial distribution method the pay-per-download service.

«swarm» of hosts to download and upload from each other simultaneously. Such swarm also includes mobile phones as well as all devices that are able to efficiently distribute files to many recipients. In order to download a file, a tracker site is though necessary, as it regularly serves as index of all links where the file can be found, even though, once the download is initiated there is no need to be in contact with a tracker site anymore. The «revolution» of BiTorrent protocol lies in its being open source software, therefore available as an open standard: torrent files do not depend on tracker sites but, given the open nature, they can interact with any tracker site in the world. This has defeated all the legal actions that have been undertaken against the many PirateBay sites[19] and, needless to say, even third generation P2P networks are ad-based models.

2.2. The advertisement-based distribution and the rise of streaming

The main feature of the first phase of online distribution of digital content above analysed revolves around *downloading* as the distribution method adopted within both DMSs and P2P networks[20]. Meanwhile, as to the revenue system adopted, legal distribution models were mainly based on payment –either per-download or via subscription– while illegal distribution models started relying on advertisement.

However, as it is well-known, ad-based distribution did not just stay with P2P networks for long, as even in the realm of legal distribution, revenue system models based on licensing were soon joint by those based on advertisement. Although the latter were initially overlooked, as it was believed that the return generated by the sale of advertising could never equal what generated by the sale of music files using DRM systems to control –at least from a theoretical point of view– their access and use, market figures overcame this believe and ad-based distribution models have increasingly been employed.

Among the first legal distributors to implement an ad-based revenue model was Mjuice which sold banner and virtual room for commercials on its webpages[21], while the Internet Underground Music Archive tried to include commercials in the files offered for streaming[22]. Neither of these businesses, though, matched the apparent success of We7[23], which was

19 Kevin Bauer, Dirk Grunwald, Douglas Sicker, *The Arms Race in P2P*, (August 15, 2009). TPRC 2009. Available at SSRN: http://ssrn.com/abstract=1997789 (discussing the rightholders' tactics and users' responce in the BiTorrents fight).

20 Seth Ericsson, *The Recorded Music Industry and the Emergence of Online Music Distribution: Innovation in the Absence of Copyright*, in 79 *The George Washintgon Law Review*, 1783, 1789 (2011).

21 The service offered by Mjuice has been suspended and afterword the website has been closed.

22 The Internet Underground Music Archive is no longer available. For an archived version of the site, please see http://web.archive.org/web/*/http://www.iuma.com.

23 We7 Homepage, http://www.we7.com. The service was launched in May 2007, with initially only 30 tracks available to users which the year after had expanded to over 3 million downloads and over 100,000 subscribers and, in the upstream market, had managed to license music from some of the world's leading artists, record labels and distributors.

made popular by the fact of being the first to permit the choice between streaming and downloading of music for free with advertisements, or the purchase/download of music files without advertisement[24].

As far as the market for online distribution of digital content evolves, streaming emerges as the distribution method that coupled with an ad-based revenue system enables many different services. Indeed, streaming is endorsed by a various number of distributors, ranging from traditional DMSs (such as iTunes), to webradios (such as Pandora), to portals (such as Yahoo), to social network (such as MySpace)[25]. To the extent that the term «ad-supported streaming» was coined as streaming was thought to replace downloading[26].

Streaming has resulted in a successful method of distribution even on the illegal side of online distribution, although downloading still continues to offer a valid method for the unauthorized fruition of digital content. Moreover, the combination of streaming and ad-based revenue lies at the heart of the new phenomenon of UGC platforms whose function, though, is not that of offering access to illegal content, rather, of aggregating content derived from users[27]. In a way, UGC platforms not only constitute a further method of distribution, but also contribute to enlarge the amount of content available online.

---

24 We7, How it works, http://www.we7.com/#/about/how-it-works.
This distribution model is enabled by the MediaGraft technology which places advertisements at the beginning of each track streamed or downloaded for free. The We7 service allows users to remove the advertisements from downloads after four weeks.

25 A second line of studies, carried by the Institute for Information Law at the University of Amsterdam, highlights the emergence of streaming and how it is intertwined to ad-based model of revenue. Cfr. Hugenholtz, Van Eechoud, Van Gompel et al., *The Recasting of Copyright & Related Rights for the Knowledge Economy*, Final report, Institute for Information Law, University of Amsterdam, The Netherlands, 2006, http://www.ivir.nl/publications/other/IViR_Recast_Final_Report_2006.pdf; Guibault, Westkamp, Rieber-Mohn, Hugenholtz et al., *Study on the implementation and effect in member states' laws*, Final Report, Institute for Information Law, University of Amsterdam, The Netherlands, 2007, http://www.ivir.nl/publications/guibault/Infosoc_report_2007.pdf; Helberger, Guibault, Janssen, Van Eijk, Angelopoulos, Van Hoboken, Swart et al., *User-Created-Content: Supporting a participative Information Society*, Final Report, Study carried out for the European Commission by Idate, Tno and IViR, 2008, http://www.ivir.nl/publications/helberger/User_created_content.pdf; Huygen, Rutten, Huveneers, Limonard, Poort, Leenheer, Janssen, Van Eijk, Helberger, *Ups and downs. Economic and cultural effects of file sharing on music, film and games*, TNO-rapport, http://www.ivir.nl/publicaties/vaneijk/Ups_And_Downs_authorised_translation.pdf

26 On the lack of substitution between downloading and streaming, see Dang Nguyen, Godefroy, Dejean, Sylvain and Moreau, François, Are Streaming and Other Music Consumption Modes Substitutes or Complements? (March 16, 2012). Available at SSRN: http://ssrn.com/abstract=2025071

27 For a first description of the «social network» phenomenon see Boyd, Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 Journal of Computer-Mediated Communication, 210, 211, (2007). Besides the generalist platforms such as MySpace, Facebook, Skyrock, Bebo, Netlog, Hyves, StudiVZ.de, Piczo, Zap.lu, MSN, Giovani.it, Arto.dk, Yahoo, One.lt, Grono, Tuenti, Aha.

Facebook, MySpace, Friendster, and Xanga are among the first social network websites that rely on UGC to attract and obtain revenue primarily from the sale of online display advertising, while it is worth noting that UGC platform incomes seem to be generated also through the accumulation of user information, which use for targeted marketing purposes is highly controversial[28, 29].

Both UGC and social network sites present elements that are highly debated and require analysis in terms of the business models implemented as well as the content posted and disseminated. As far as the entrepreneurial activity and the business models are concerned, it is worth mentioning that social network members are both «content providers» and «customers» of the website as their exposure to advertising while using the platform generates revenue. In 2006 MySpace was the fifth most popular web domain (behind Google, Yahoo, MSN, and AOL) in total number of individual pages and served 8% of all advertisements on the Internet[30].

At the moment it is Facebook to present the business model most relying on advertising. Because of its deep penetration within a series of micro communities (e.g., college campuses), since the beginning this platform has enabled local advertisers to use Facebook to target specific colleges or other audiences[31]. Facebook «social ads», for example, are not only a very specific tool to target customers, but can also leverage the power of «Facebook News Feed» by updating all the contacts of a user that shows interest in a specific product[32]. However, the economic sustainability of the UGC platforms is not only derived from the

---

bg, we can find «content-based» platforms that are used to upload and access UGC such as Youtube, Dailymotion and Flickr, «business networks» such as LinkedIn and Ecademy, and «micro-blogging network» such as Twitter (see http://ec.europa.eu/information_society/activities/social_networking/facts/index_en.htm).

28 *See* Michael Trusov, Randolph E. Bucklin & Koen Pauwels, *Effects of Word-of-Mouth versus Traditional Marketing: Findings from an Internet Social Networking Site* (Working Paper Series, Apr. 24, 2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1129351.

29 It is worth mentioning that UGC platforms not only provide hints on the users' trends (and by doing this they generate value for marketing operators), but they constitute an asset by themselves (*See* Elkin-Koren, *User-Generated Platforms*, in Working Within the Boundaries of Intellectual Property, R. Dreyfuss et al. eds, at 114-15).

30 Yinka Adegoke, *MySpace to Sell Music from Nearly 3 Million Bands*, Boston.com Business, Sept. 1, 2006, http://www.boston.com/business/technology/articles/2006/09/02/myspace_to_sell_music_from_nearly_3_million_bands/; Dan Smith, *Online Social Networks & Communities are Here to Stay*, Know More Media, Sept. 22, 2006, http://www.knowmoremedia.com/2006/09/online_social_networks_communi.html.

31 Nisan Gabbay, *Facebook Case Study: Offline Behavior Drives Online Usage*, Startup Review, Nov. 5, 2006, http://www.startup-review.com/blog/facebook-case-study-offline-behavior-drives-online-usage.php.

32 *See Facebook Unveils Facebook Ads*, 6 novembre 2007, http://www.facebook.com/press/releases.php?p=9176.

sale of advertising. This is combined with income from other sources such as subscriptions, donations, licensing and e-commerce[33].

As to the nature of content distributed, there have been cases against UGC platforms aiming at affirming their involvement in the illegal fruition of copyright infringing materials. However, differently from the cases above mentioned, the model herein adopted does not trigger the intermediary's liability as long as a notice and take down procedure has been implemented by the platform.

3. CLOUD-BASED MUSIC SERVICES AS NEW MODEL OF MUSIC DISTRIBUTION

As seen, following the digitalization of music and the phenomenon of illegal file-sharing, renewed schemes for music distribution have become urgent needs. Yet, while phasing in the problem of illegal fruition of copyright content and suggesting new business models for the music industry, we have entered a new era in computing where, increasingly, people access and share information through the use of remote server networks, instead of doing it with their own personal computers and IT systems, and music contents are relentlessly drawing into this recent trend as well[34]. Thus, in the following subsections the phenomenon of cloud computing as well as its application to the online distribution of music will be taken on.

3.1. The nature of cloud computing

The incipient ideas of this emerging way of delivering computing resources known as cloud computing are not properly new and dates back to 1965 when the company Western Union set the ambitious plan for acting as an «information utility»[35]. However, against this

---

33 Helberger N., Guibault L., Janssen E. H., Van Eijk N., Angelopoulos C. J., Van Hoboken J., Swart E. et al., *User-Created-Content: Supporting a participative Information Society*, *supra* note 25, at 115.

34 The move to the cloud is driven by the use of many different devices to access data and applications. Today smartphones are the drawing force as a result of the desire of the marketplace to be mobile, also due to the currently blurred boundaries between smartphones and computers: J.Q. Anderson and L. Rainie, *The Future of Cloud Computing,* Pew Research Center Series, at 10-11 (2010), http://www.workingtitleconsultants.com/wp/wp-content/uploads/2010/06/The-future-of-cloud-computing.pdf. In the next future many more different types of networked appliances will assume this function. It is maintained that cloud computing might have a great potential for the «Internet of the things» where everyday objects have their own IP addresses and can be tied together by the cloud: *see* E. Braathe, *Internet of Things and Cloud Computing,* IBM Workshop Paper, (2010), http://www.rfidrnet.com/Presentations_11_May_2010/E_Braathe_IBM_Workshop_IoT_Oslo_11_May_2010.pdf; T. Silva, *Is Internet of Things and Cloud Computing Like Romeo and Juliet?.* http://www.blog.telecomfuturecentre.it/2011/02/20/is-internet-of-things-and-cloud-computing-like-romeo-and-juliet/.

35 More precisely, within its 1965-plan, the telegraph company Western Union planned to become «a nationwide information utility, which will enable subscribers to obtain, economically, efficiently, im-

early definition, the novelty about cloud computing mostly, though not only, lies in its role as solver for web-scale problems, and then, in how cloud computing permeates a multitude of Internet activities nowadays[36]. First of all, on the «enterprise cloud» side, the growing demand of computing capacity for electronic data processing by organisations has been met by technology companies which build large data centres, and then, offer this infrastructure as a service («IaaS») to enterprises who are able to reduce capital investments in physical infrastructure thanks to the consolidation of such great number of servers[37]. Likewise, enterprises are taking advantage of development platforms in the clouds offered as services («PaaS») and devoted to the creation of web applications[38].

On the «consumer cloud» side instead, users of cloud computing are allowed to store, access and share information they need anytime, wherever they are, from any networked device without loading any software on their own hardware. Indeed, SaaS (Software as a Service) is a multitenant model where physical hardware infrastructure is shared among many different users, though is able to differentiate data belonging to each tenant, and customers rent software for use[39]. Moreover, cloud computing for consumers also refers to a common activity carried out by web-surfers as storing content into Internet services run for a specific

---

mediately, the required information flow to facilitate the conduct of business and other affairs», *see* The Future Role of Western Union as a Nationwide Information Utility, Company Strategic Plan, 1965, Western Union Telegraph Company Records 1820-1995, National Museum of American History, Smithsonian Institution, Washington. D.C., 1965 at http://www.governmentattic.org/2docs/WesternUnionStrategicPlans_1965.pdf>.

36 In the business arena, the migration to cloud computing services also aims to enhance productivity since easing the integration of multiple applications or collaboration suites: *see* Techrepublic for Google, *Cloud Computing: Latest Buzzword or a Glimpse of the Future?* (2011) http://www.techrepublic.com/whitepapers/cloud-computing-latest-buzzword-or-a-glimpse-of-the-future/1130967.

37 Organizational users, ranging from big corporations to SMEs and governments, may benefit from the IaaS model of cloud computing not only for the cost-saving leverage but also in terms of wider economic, ecological and technical advantages. *See, e.g.,* N. Tsilas, *Moving Responsibly to the Cloud to Ensure Its Full Potential,* 27 The Computer & Internet Lawyer 16 (2010) on the pro-competitive effect of cloud computing for small businesses since giving the same computing capacity that only largest corporations had before. *See also* Enisa (European Network Security Agency), *Cloud Computing: Benefits, Risks and Recommendations for Information Security* (2009), at 17-19, pointing out that while there are a few security dangers in the cloud, there are also significant advantages.

38 In this way organisations can create web applications without installing tools on their computers and without any specialized administration skills. The most known examples of PaaS include Google App Engine and Amazon Web Services.

39 The earliest examples of SaaS in the consumer space have been email services such as Gmail and Hotmail. Then, Google and Microsoft have consolidated their positions in the cloud computing business with other services, like Picasa and Youtube for the former, or Office 365 which brings online the Microsoft Office suite.

purpose, like Flickr for photos, or Google Docs for documents and applications[40]. Although there is a diversity of opinion on what exactly cloud computing is, the performance of computing and communicating activities carried out by individual users of the consumer cloud through any of their web connected devices is certainly included into the definition of this nebulous term[41].

As such, some of the most popular websites are cloud-based, like webmail services or social networking sites. In the mind of the user, these online services are not computing activities but rather daily actions like shopping, banking or being entertained. According to the Internet companies' perspective, these are cloud-supported services enabled by cloud computing and consisting in technology development and process management of data belonging to their websites' users.

This does not mean that personal software and hardware are going to disappear, however the technology literature sees a «hybrid life» in the next years where the evolution of desktop and cloud-based computing will proceed in tandem, in order to combine the well-rendered attributes of cloud computing, such as scalability, elasticity and, most of all, cost effectiveness[42], with a number of unsolved problems related to security and the Net access dependence of cloud computing[43].

3.2. The changing shape of digital music in the Cloud

Contemporary landscape of the Internet music services reflects such hybrid character of computing activities as split between desktop and cloud-based computing, and the move

40 Many people are already using the cloud every day, even though they are not aware of it. A Pew Internet Data Memo of 2008 supported this point reporting that 69% of US citizen had either stored data online or used cloud-based applications at least once: *see* J.B. Horrigan, *Use of Cloud Computing Applications and Services,* Data Memo, Pew Internet and American Life Project (2008) http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services/Data-Memo.aspx.

41 Many times a certain definition of cloud computing simply mirrors a specific focus over this extensive change in information technology. Instead, it worth considering the significant distinction between cloud services and cloud computing as such. Whereas the former category encompasses individual and organizational solutions that are delivered and consumed in real-time over the Internet, the latter hints at an IT delivery model enabling real-time delivery of solutions like cloud services: *see* F. Gens, *Defining «Cloud Services» and «Cloud Computing,* http://blogs.idc.com/ie/?p=190 (last visited March 26, 2012).

42 S. Marston et al., *Cloud Computing – The Business Perspective,* 51 Decision Support Systems 176 (2011), identifying a definition as well as opportunities and challenges from the business side of cloud computing.

43 For a well explained analysis of organisational, technical and legal risks of cloud computing, *see* Enisa, *supra note* 37. A 2010 survey of 895 technology stakeholders and critics reported their expectation for a more sophisticated desktop-cloud hybrid with improved ways of interaction between the two computing forms: *see* J.A. Anderson and L .Rainie, supra note 34.

towards digital clouds signals a fundamental shift also in how music is distributed inside the online environment.

During these last years the significance of music as a commodity changed as a consequence of the changes in the technologies for its production and distribution. Technological innovation is disruptive since it challenges traditional business models and old regulatory frameworks, and so it induces to new economies. Digital technologies enable consumers to download files in readiness insomuch as they are allowed to gather and share creative contents on a large scale.

The Napster case demonstrated that traditional business models adopted by the entertainment industry gradually lose economic effectiveness when translated to the digital environment. Further, the Net has permitted new ways to communicate and spread ideas and, accordingly, it has moulded social interaction. The development of social networking sites like MySpace revealed the existence of alternative avenues for developing music culture and its products. Music itself is renovating its role since becoming something ephemeral whose duration is notably compressed and less bound to one particular material expression[44]. Indeed its consumption does not require physical recording anymore as exemplified in the success that music streaming has achieved in current business models for online distribution. Today, music can be directly conveyed from the Internet to multiple devices and its packaging may assume so many forms that it has gained a different way of distribution and consumption through cloud-based music services. Technology keeps moving and currently we are entering the digital convergence stage, a trend originated by a new generation of multitasking portable devices and permitting further disintermediation. While the initial dyad iTunes-iPod still needed a computer to download music, currently smartphones are capable to download music directly through WiFi connection together with listen to music, phone people, send emails, take pictures, surf the web or search for places. High speed wireless networks permit such expeditious netsurfing and the proliferation of mobile devices empowers individual users to get to the Internet without being tied to a physical location[45]. A recent survey of Foreign Policy over the Net reports that the biggest «game changing» Internet-related technology in the next future is mobile technologies. Mobile devices features offer tremendous opportunities for customers who may stay connected 24/7 and so consider Internet facilities as part of their daily lives[46].

According to the same survey, cloud computing is the other big promise within the Internet realm as it will play an essential role in the way we access to information and, at least for the consumer cloud side, its rise is very connected to the proliferation of web-connected

44 B. Cammaerts and B. Meng, Creative Destruction and Copyright Protection: Regulatory Responses to File-Sharing, London School of Economics and Political Science, Department of Media and Communications, Media Policy Brief 5 (2011).

45 J.B. Horrigan, *Seeding the Cloud: What Mobile Access Means for Usage Patterns and Online Content,* Pew Internet & American Life Project (2008), http://pewinternet.org/~/media//Files/Reports/2008/PIP_Users.and.Cloud.pdf.pdf.

46 Foreign Policy, *The FP Survey: The Internet,* (2011) http://www.foreignpolicy.com/articles/2011/08/15/the_fp_survey_the_internet.

devices. In other words, latest technologies are driving to a more distributed computing environment and, at the same time, to a centralized storage. The improvement of broadband connection, the decreasing cost of storage and the spread of handheld devices like smartphones and tablets entail that users can constantly access the data stored in the cloud from their own computer, someone else's computer or a mobile device.

Music is included in this variety of data stored in cyberspace and accessed through cloud-based applications. The common idea of cloud music services is that fruition of music can be done through the cloud, though differences exist as for the operational modes for doing it. On the one hand, music streaming services, also in their renewed form of music social networking sites such as Spotify and SoundCloud, provide access to music stored in the private cloud of the website[47]. On the other, music locker services (MLSs) such as Google Music and Amazon Cloud Drive pursue a storage strategy which entails the provision of a personal cloud to the user[48] for her files, which she can access wherever there is a web connection. More correctly, this distinction represents the two pure models of cloud-based music services but it worth clarifying that the actual offer by Internet companies is more and more mixed, so much so today a single website may allow all these different uses.

In fact, while the early music services like Pandora just let access to Entrepreneurial Generated Content (EGC) via streaming, nowadays the most popular music sites count on an integrated offer which, other than allowing users to stream music, has new features such as easy sharing of playlists with friends and personal library streaming. For providing such additional services, frequently the music websites rely on the cloud computing architecture, even if they do it differently and according to the specific characters of their site as well as the type of activities that they want to let users to perform. In general, what can be detected as a trend in the music distribution landscape is the growing provision of locker-alike services from online music platforms that are not pure music locker sites, but acquire new features on the wake of the emergence of proper MLSs,, and by doing this they aim at complementing their core business. For instance, scrutinising the popular website Spotify, which typically provides access to tracks from major and independent labels thanks to streaming technologies, a gradual improvement of its service with numerous upgrades can be observed, including social networking features and a web/desktop hybrid music player which also permits to upload any iTunes library stored in one computer to Spotify in order to access it everywhere. The same is done by Sony Music Unlimited which, regardless the subscription level, offers the opportunity to match all the songs owned by its users and their playlists in order to import them into a cloud library. However, there is also a parallel trend triggered by

47 P. Mell and T. Grance, *The NIST Definition of Cloud Computing: Recommendations of the national Institute of Standards and Technology,* NIST – US Department of Commerce, Special Publication 800-145 (2011) defining the private cloud as the cloud infrastructure provisioned by a cloud provider to a single organization who make it available to multiple consumers.

48 Y. Tian, B. Song and E-N Huh, *Towards the Development of Personal Cloud Computing for Mobile Thin-Client',* International Conference on Information Science and Applications (2011) where among the types of personal cloud is cited the online storage.

the rise of file-hosting sites (i.e. sites providing repositories for personal content that enable users to access it from whatever device the users choose) and leading to the creation of hosting services tailored to music content. From general-purpose cyberlockers like DropBox we have shifted to more definite websites whose services are refined according to their targeted customers and iCloud or Google Music simply represent the bulk of the iceberg.

This terrific development, herein analysed as for music distribution, can be read as the shift «from being device-centric to information-centric»[49]. The file-hosting service becomes a tool both for work and personal life since it is a much more convenient way for transferring files than sending them as email attachments, not to mention how it eases the access to them from multiple devices without the need of annoying uploads. Either grounded on ad-based or subscription models, both general-purpose and specialized cyberlockers offer hard drive space online to store personal files and the opportunity to share these hosted files with other people who are sometimes known and some other times not.

Nonetheless, cyberlockers raise also concerns as the next battleground for copyright suits, and because of the use, and perhaps at times the abuse, of their hosting and sharing functions. As for the hosting feature, for example, the music locker service MP3tunes has been recently sued by EMI label for its storage method. In order to reduce the amount of disk space needed per user, MP3 tunes' software checks whether a user's library matches with previously uploaded songs by other users, and, in that case, the track is added to the cloud without effectively uploading it. In other words, MP3tunes keeps just one single copy of that song regardless how many users have it in their individual lockers. The «single storage method» has been brought before the New York Federal Court and the ruling of the last August made clear that this practice is legal provided that «the system preserves the exact digital copy of each song uploaded to MP3tunes.com». This means that MP3tunes cannot substitute any uploaded song with a master copy but, quite the opposite, it has to store all the different files of a same song as determined by an MD5 Hash. Meanwhile, Judge William H. Pauley III in the MP3tunes case also ruled about «sideloading», a function integrated into the MP3tunes services which permits users to add tracks that have been downloaded from links available on webpages, like blogs, directly to their online locker. Regarding this aspect, Judge Pauley ruled that this practice is legal as long as the site removes links and songs added to lockers when a copyright holder send a notice informing that such links infringe their copyright[50].

Even though the New York Federal court established that the single storage method is the right way to supply online hosting services, other providers of music locker services like

49 Simran, *Microsoft Goes in Hard as Software War Heats Up with Google* (2010), *see* http://onlysoftware-blog.com/2010/09/microsoft-goes-in-hard-as-software-war-heats-up-with-google/

50 The wide significance of sideloading for cyberlockers has been recently demonstrated by the choice made by the established hosting site Dropbox to add this function to its services; see, http://blog.dropbox.com/?p=1138. Even though this specific feature is more about streaming the content via the link, and not downloading, it clearly reminds the Megavideo model which used to offer access to content without necessarily downloading it.

Amazon and Google decided to require every user to upload every song. Considering the inherent drawbacks of this choice like the extended bandwidth usage and length of the upload, the reason may lie in the fact that a single decision is not enough to dissipate worries about copyright infringements. Only Apple's new music service iCloud applies the single storage method introduced by MP3 tunes and, even more, it uses master copies. Thanks to a long-awaited agreement with major labels, in case iCloud customers have low quality copies of a song, Apple is entitled to automatically upgrade that song to a better version[51].

Whereas the MP3tunes ruling mainly attracted attention as for the storage method part, the other aspect of sideloading is also relevant since representing the meeting point of the concerns connected to the storage function with the ones deriving from the sharing function. Even if cyberlockers can be used for legitimate purposes, such as storage space for one's own creations and for personal library streaming, they are also known for being used as repository of infringing copyright content. Although hosting sites do not feature search capabilities, it is not hard to discover «link sites» like blogs helping users to find shared music files hosted on cyberlockers. In MP3Tunes, Judge Pauley, while focusing on the sideloading aspect of the relationship between cyberlockers and link sites, acknowledged that the liability for copyright infringement of the hosting site ends when it complies with the notice and take down procedure set by the DMCA.

This clarification pertaining to the second typical function of cyberlockers, that is the sharing feature, is an important point of reference for hosting sites that actively encourage users to store files. While cyberlocker sites include disclaimers about compliance with the DMCA as well a notice and take down process, their incentive programs are under the scrutiny of copyright holders and, since a few months, of the judicial bodies too. Megaupload, one of the most popular cyberlocker sites that has been closed via the seizing of its domain names, the grabbing 50 million dollars in assets, and the arresting by New Zealand police of four site's key employees including the founder Kim Dotcom, offered a premium account to users who gained credits for the amount of uploads. However, scrutinizing such incentive programs should consider that cyberlocker sites' policy usually requires to declare that the uploaded content is not protected by copyright. Therefore the encouragement of uploading by offering incentives does not necessarily imply the uploading of infringing content.

4. A NEW PHASE FOR ONLINE DISTRIBUTION OF DIGITAL CONTENT: CONCLUDING REMARKS

The scenario so far depicted has acquired complexity over the different phases of online distribution of digital content and the emergence of music services relying on cloud computing architecture does not help to clear the picture.

51 http://www.wired.com/epicenter/2011/08/cloudmusic-is-not-a-crime/.

First, we observed that while legal distribution is characterized by a stable trend toward centralized models for distribution, illegal distribution models started from a centralized mode Napster-alike and evolved toward decentralized modes. With the advent of cloud-based services both legal and illegal sides of music distribution converge toward a model that is at the same time centralized/decentralized: a dichotomy that springs out from the «centralization of storage» and the «decentralization of access». As a matter of fact, storage is in the hand of Internet companies that offer locker services, while access is allowed to diverse individuals and through multiple devices.

In this scenario, the similarity with the former models lies in the fact that centralization and decentralization still coexist, but, and here lies the dissimilarity, they coexist in a very different way. In other words, while in the previous model it was the content as such to be decentralized and the access points were just computers, now the access points to content are decentralized among a multitude of different devices and the content resides on a single place, that is the cloud provider's servers. Consider, for example, the decentralized nature of BiTorrent files as opposed to the current centralized nature of content stored on Google Music, together with its availability.

As a consequence of the different combination between centralization and decentralization, users acquire enhanced access to information stored, but decrease the control over it in terms of availability. Meanwhile, cloud providers control availability but not the nature of the content stored. In other words, a feature in the future of online distribution is likely to be the dispersion of control over content stored in the cloud, both in terms of availability and compliance with copyright law[52].

Second, downloading and streaming models turn out not to be substitute distribution systems, and the underlying business models neither. It seems relevant to recognize the lasting difference in the level of control and access over content that is conferred by downloading. On the one hand, since ownership still matters even in a dematerialized form, and bandwidth availability and speed remains a thorny problem to address, it is not hard to understand the reason behind the propensity of users to still download music anyway. On the other hand, streaming technology may permit both a prompt availability of the content –without waiting for the time of downloading– and the extended availability of downloaded content since enabling the access from multiple devices. These different features have gradually driven to several combinations of downloading and streaming facilities within the online music sites so much so the two technologies rise to be complementary. In practice the divergences in their technical combination are the result of the different business model adopted by websites, which may decide to differently rest on ad-based, subscription and pay-per-download revenues.

52 The MegaUpload Saga is also showing this intricate relation between control over data and copyright infringement; see http://www.techdirt.com/articles/20120403/03211918344/mpaa-says-letting-anyone-access-data-megaupload-servers-would-represent-infringement.shtml.

Third, also and specially for cloud-based services, the business models grounded on advertisement are increasingly source of concern for data protection issues. Indeed, even when data mining operations are carried out by websites in order to improve services like web recommendations and «predictions» of content that users might like to get, then this personal information may be used for other, unpredicted, purposes like behavioural and semantic advertising.

Finally, regarding the conditions under which the liability for copyright infringement is alleged by the right holders toward websites, we have found the recurrent element of the incentive-to-share, either monetary or in terms of credits for premium accounts, under scrutiny in the recent lawsuits involving cyberlockers.

Taken together, all these courses of action contribute to show the likely boundaries that online legal distribution of music will develop in the next years. Indeed, judicial rulings covering current, and perhaps incoming, copyright disputes around some of the key features of cloud-based locker sites, and the services supplied by them, will provide an essential roadmap for defining what of their new ways for content delivering amount to copyright infringement. As a result, in case copyright regimes will not be able to accommodate these novel potentialities offered by cloud computing, the foreseeable scenario is their exclusive appropriation by the illegal alternatives for online music distribution. Hence, as for the sideloading aspects of locking websites, future models of MLSs could be affected by any court decision about the legality of links to external contents, and more, whether differences between the links enabling content download and those permitting streaming will be detected.

Moreover, the negotiating power belonging to locker sites is going to constitute another essential detail in the future image of online music distribution. In fact, despite the ruled unlawfulness of the «master copy method» adopted by certain MLSs, we have already experienced how Internet companies can overcome the hurdle through private negotiations with music labels, and eventually gain the opportunity to offer this type of service to their customers. Meanwhile, other sites that cannot enter into similar deals have only the option to frame their business models within the boundaries set by the law, and so limiting the size of their services, or to decide riding the weave of online music distribution outside the law.

We can speculate that the same is expected to happen with regard to the incentive programs embraced by some music sites. Different sort of sharing revenue systems are spreading over the Net, but bound together by the common goal of incentivizing content uploading by the users. While the incentive element has been typically deemed as a clue of copyright infringement – typically in P2P case but, quite recently, also in the dispute involving the popular cyberlocker MegaUpload, it also acts as a building block of articulated business models laid down by the most important players of the Internet, and with the consent of the copyright holders.

As a consequence, any online music site that is willing to add music locker features to its services might face strong difficulties to define a long-term strategy, and then, it will be eventually deterred from inserting them. Unfortunately, the uncertainties around copyright law interpretation and application are at the heart of this problem and they provide a further

demonstration about how traditional copyright rules are not fit for the digital environment, and the reasons behind the urgent need of their reform.

5. BIBLIOGRAPHY

Adegoke Y. (2006). *MySpace to Sell Music from Nearly 3 Million Bands*. Boston.com Business. Retrieved March, 25th, 2012, from http://www.boston.com/business/technology/articles/2006/09/02/myspace_to_sell_music_from_nearly_3_million_bands/.

Anderson J.Q. and Rainie L. (2010). *The Future of Cloud Computing,* Pew Research Center Series. Retrieved March, 25th, 2012, from http://www.workingtitleconsultants.com/wp/wp-content/uploads/2010/06/The-future-of-cloud-computing.pdf.

Armstrong, J.R. (2003). Sony, Napster, and Aimster: An Analysis of Dissimilar Application of the Copyright Law to Similar Technologies. *DePaul-LCA J. Art & Ent. L. & Pol'y*, 13, 1.

Bauer, Grunwald, Sicker. (2009). *The Arms Race in P2P*. Retrieved March, 25th, 2012, from http://ssrn.com/abstract=1997789.

Boyd, E. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication,* 13, 210.

Braathe, E. (2010). *Internet of Things and Cloud Computing,* IBM Workshop Paper, http://www.rfidrnet.com/Presentations_11_May_2010/E_Braathe_IBM_Workshop_IoT_Oslo_11_May_2010.pdf.

Cammaerts, B. and Meng, B. (2011). Creative Destruction and Copyright Protection: Regulatory Responses to File-Sharing, London School of Economics and Political Science, Media Policy Brief 1.

Choi, B.H. (2005-06). The Grokster Dead-End. *Harv. J. L. & Tech.,* 19, 393.

Elkin-Koren. (2010). User-Generated Platforms. In R. Dreyfuss et al. (eds.), *Working Within the Boundaries of Intellectual Property,* (pp. 114-15). New York: Oxford University Press.

Enisa (European Network Security Agency). (2009). *Cloud Computing: Benefits, Risks and Recommendations for Information Security*.

Ericsson S. (2011). The Recorded Music Industry and the Emergence of Online Music Distribution: Innovation in the Absence of Copyright. *The George Washintgon Law Review*, 79, 1783.

Ficsor, M. (2002). The Law of Copyright and the Internet. New York: Oxford University Press.

Fisher, Gasser, Slater, Smith, Palfrey (2005). *Comments on the OECD Working Party on Information Economy Draft Report «Digital Broadband Content: Music»*, Berkman Center for Internet & Society at Harvard Law School. Retrieved March, 25th, 2012, from http://cyber.law.harvard.edu/digitalmedia/oecd_comments.pdf.

Foreign Policy. (2011). *The FP Survey: The Internet.* Retrieved March, 25th, 2012, from http://www.foreignpolicy.com/articles/2011/08/15/the_fp_survey_the_internet.

Gabbay N. (2006). *Facebook Case Study: Offline Behavior Drives Online Usage*, Startup Review. Retrieved March, 25th, 2012, from http://www.startup-review.com/blog/facebook-case-study-offline-behavior-drives-online-usage.php.

Gasser et al. (2004). *iTunes How Copyright, Contract, and Technology Shape the Business of Digital Media. A Case Study*. Retrieved March, 25th, 2012, from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/GreenPaperiTunes041004.pdf.

Gasser, McGuire. (2005), *Copyright and Digital Media in a Post-Napster World: International Supplement*, Retrieved March, 25th, 2012, from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/wpsupplement2005_0.pdf.

Gasser, Ruiz Begue, (2005). *iTunes: Some Observations After 500 Million Downloaded Songs*. Retrieved March, 25th, 2012, from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/iTunes_August_update_final[1].pdf.

Gasser, Slater, Smith, Palfrey, Locke, McGuire (2005) *Copyright and Digital Media in a Post-Napster World*. Retrieved March, 25th, 2012, from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2003-05.pdf.

Gasser, Slater, Smith, Palfrey, Locke, McGuire (2005) *Copyright and Digital Media in a Post-Napster World*, *Version 2*. Retrieved March, 25th, 2012, from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/wp2005.pdf.

Gasser, Slater, Smith, Palfrey, Locke, McGuire. (2003). *Five Scenarios for Digital Media in a Post-Napster World*. Retrieved March, 25th, 2012, from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2003-07.pdf.

Gens, F. *Defining «Cloud Services» and «Cloud Computing,* Retrieved March, 26th, 2012, from http://blogs.idc.com/ie/?p=190.

Guibault, Westkamp, Rieber-Mohn, Hugenholtz et al. (2007). *Study on the implementation and effect in member states' laws*, Final Report, Institute for Information Law, University of Amsterdam, The Netherlands. Retrieved March, 25th, 2012, from http://www.ivir.nl/publications/guibault/Infosoc_report_2007.pdf;

Helberger, Guibault, Janssen, Van Eijk, Angelopoulos, Van Hoboken, Swart et al. (2008). *User-Created-Content: Supporting a participative Information Society*, Final Report, Study carried out for the European Commission by Idate, Tno and IViR. Retrieved March, 25th, 2012, from http://www.ivir.nl/publications/helberger/User_created_content.pdf.

Horrigan, J.B. (2008). *Seeding the Cloud: What Mobile Access Means for Usage Patterns and Online Content,* Pew Internet & American Life Project. Retrieved March, 25th, 2012, from http://pewinternet.org/~/media//Files/Reports/2008/PIP_Users.and.Cloud.pdf.pdf

Horrigan, J.B. (2008). *Use of Cloud Computing Applications and Services,* Data Memo, Pew Internet and American Life Project. Retrieved March, 25th, 2012, from http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services/Data-Memo.aspx.

Hugenholtz, Van Eechoud, Van Gompel et al. (2006). *The Recasting of Copyright & Related Rights for the Knowledge Economy*, Final report, Institute for Information Law, University of Amsterdam, The Netherlands. Retrieved March, 25th, 2012, from http://www.ivir.nl/publications/other/IViR_Recast_Final_Report_2006.pdf.

Huygen, Rutten, Huveneers, Limonard, Poort, Leenheer, Janssen, Van Eijk, Helberger. *Ups and downs. Economic and cultural effects of file sharing on music, film and games*, TNO-rapport. Retrieved March, 25th, 2012, from http://www.ivir.nl/publicaties/vaneijk/Ups_And_Downs_authorised_translation.pdf.

Marston S. et al. (2011). Cloud Computing – The Business Perspective*, Decision Support Systems*, 51 176.

McGuire, Slater, *Consumer Taste Sharing Is Driving the Online Music Business and Democratizing Culture*. (2005). Retrieved March, 25th, 2012, from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/11-ConsumerTasteSharing.pdf.

Mell P. and Grance T. (2011). *The NIST Definition of Cloud Computing: Recommendations of the national Institute of Standards and Technology,* NIST – US Department of Commerce, Special Publication 800-145.

Mori, Kawahara. (1990). *Superdistribution. The Concept and the Architecture*, The Transactions Of The Ieice, 73, 1133. Retrieved March, 25th, 2012, from http://www.virtualschool.edu/mon/ElectronicProperty/MoriSuperdist.html.

Nguyen, Godefroy, Dejean, Sylvain and Moreau, François. (2012). *Are Streaming and Other Music Consumption Modes Substitutes or Complements?.* Retrieved March, 25th, 2012, from http://ssrn.com/abstract=2025071

Rosenblatt, B. (2004). *Learning from P2P: Evolution of Business Models for Online Content*, INDICARE. Retrieved March, 25th, 2012, from http://www.indicare.org/tiki-read_article.php?articleId=61.

Silva, T. (2010). *Is Internet of Things and Cloud Computing Like Romeo and Juliet?.* Retrieved March, 25th, 2012, from http://www.blog.telecomfuturecentre.it/2011/02/20/is-internet-of-things-and-cloud-computing-like-romeo-and-juliet/.

Simran, (2010). *Microsoft Goes in Hard as Software War Heats Up with Google*. Retrieved March, 25th, 2012, from http://onlysoftwareblog.com/2010/09/microsoft-goes-in-hard-as-software-war-heats-up-with-google/

Slater, Smith, Bambauer, Gasser, Palfrey. (2005). *Content and Control: Assessing the Impact of Policy Choices on Potential Online Business Models in the Music and Film Industries*. Retrieved March, 25th, 2012, from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/content_control.pdf.

Smith D. (2006). *Online Social Networks & Communities are Here to Stay*, Know More Media. Retrieved March, 25th, 2012, from http://www.knowmoremedia.com/2006/09/online_social_networks_communi.html.

Techrepublic for Google. (2011). *Cloud Computing: Latest Buzzword or a Glimpse of the Future?* . Retrieved March, 25th, 2012, from http://www.techrepublic.com/whitepapers/cloud-computing-latest-buzzword-or-a-glimpse-of-the-future/1130967.

Tian, Song, Huh. (2011). *Towards the Development of Personal Cloud Computing for Mobile Thin-Client',* International Conference on Information Science and Applications.

Trusov, Bucklin, Pauwels. (2008). *Effects of Word-of-Mouth versus Traditional Marketing: Findings from an Internet Social Networking Site*. Retrieved March, 25th, 2012, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1129351.

Tsilas, N. (2010). Moving Responsibly to the Cloud to Ensure Its Full Potential, *The Computer & Internet Lawyer*, 27, 16.

Zimmerman D.L. (2005). *Daddy, Are We There Yet? Lost in* Grokster-*land*. Public Law & Legal Theory Research Paper Series, Working Paper No. 05-21. Retrieved March, 25th, 2012, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=826064.

COPYRIGHT INFRINGING CONTENT AVAILABLE ONLINE NATIONAL JURISPRUDENTIAL TRENDS[1]

Federica Casarosa
European University Institute – Department of Law, Florence

ABSTRACT: In the last decades, technological developments have changed the tools through which citizens can access content allowing them also to interact and participate to the production process. The change in the way in which content is produced and distributed has challenged the old regulatory instruments used to protect producers and distributors. The battlefield here has been set in terms of copyright protection between copyright holders (content producers) and Internet service providers, as the latter provide copyright content freely over their platforms collecting advertising revenues. However, the first test that ISPs should pass to be held liable of copyright infringement is the one required by the rules regarding liability of Information Society Service Providers (ISSP) set by the E-commerce directive and implemented in the MS through national legislation. As long as an ISP can prove that its position is of a hosting provider, it can be exempted from liability also when infringing copyright material is available of its platform. In order to verify if and how national jurisprudence has framed the role and activity characterising a hosting provider and the subsequent obligations arising from such qualification, the paper will analyse the recent cases involving copyright holders and internet intermediaries in two European countries (France and Italy). The result of this analysis show that different approaches exist and new legal categories has been put forward by courts in order to update national legislation. The main elements that will be analysed are the characteristics of the notice; the obligation to monitor that is imposed to ISP, in particular as ex ante filtering activity; and, finally the internal distinction drawn within the hosting provider category.

KEYWORDS: hosting, internet intermediary, jurisprudence, liability, copyright, notice and take down, active host, passive host.

1. INTRODUCTION

In the last decades, technological developments have changed the tools through which citizens can access content, allowing them to interact and participate to the production process. If on users' side, this has been interpreted as a new form to implement freedom of expression principle; on traditional content providers' side, this new framework has triggered a general revision of the existing business models available.[2] New media brought new entrants into media market, providing for a wider variety of ways to access news, entertainment, and information in general. Thus, new media broke down the monopolistic or oligopolistic con-

1 This paper has been written within the project *"European Media Policies Revisited: Valuing & Reclaiming Free and Independent Media in Contemporary Democratic Systems"* (MEDIADEM), a European 7th Framework Project. Thanks to anonymous reviewer for comments and suggestions.

2 Benkler, Y. (2006). *The Wealth of Network*s : how social production transforms markets and freedom. New Haven [Conn.] : Yale University Press.

trol over distribution mechanisms hold by traditional media, and empowered consumers to seek and share any content.[3]

The change in the distribution mechanisms challenged the old regulatory instruments used to protect producers and distributors. The battlefield here is set in terms of copyright protection between copyright holders (content producers) and Internet service providers, which provide copyright content freely over their platforms collecting advertising revenues. However, the first test that Internet service providers (ISP) should pass to be held liable of copyright infringement is the one required by the rules regarding liability of Information Society Service Providers (ISSP)[4] set by the E-commerce directive[5] and implemented in the Member States through national legislation. As long as an ISP can prove that its role is of a hosting provider, it can be exempted from liability also when infringing copyright material is available of its platform. In order to verify if and how national jurisprudence has framed the role and activity characterising a hosting provider and the subsequent obligations arising from such qualification, the paper will analyse the recent cases involving copyright holders and internet intermediaries in two European countries (France and Italy). The result of this analysis allows a comparison of the main debated issues verifying if the level of harmonisation of national rules in terms of legislation has also been followed or not in the case-law. The main elements that will be analysed are the characteristics of the notice; the obligation to monitor that is imposed to ISP, in particular as *ex ante* filtering activity; and, finally the internal distinction drawn within the hosting provider category.

2. BETWEEN HOSTING AND SERVICE PROVISION – THE REGULATORY FRAMEWORK FOR ONLINE INTERMEDIARIES

The term ISP is a wide and general one. ISP can provide different kind of services and therefore can play a different role in the Internet framework. ISP's services can be categori-

3 Picard, R. (2011) *Digitalisation and Media Business Models*. Retrieved March, 26th, 2012 at www.mappingdigitalmedia.org.

4 See that the E-commerce directive use this terminology extending the most common term of Internet Service Providers (ISP). It is important to stress that ISSP definition (Art 2 E-Commerce directive) is wider than the ISP one, including hosting services, ecommerce merchants, social network sites, cloud computing services, mobile providers, etc.; though, it excludes TV and radio broadcasters where they do not offer individual on-demand services, taxation, competition law, the activities of notaries, gambling and privacy or data protection issues due to explict limitation of the directive remit. However, providers of noncommercial services on-line, such as the delivery of e-government services by state departments, if the state will be making economic gains out of the activity are included in the regime. See more in Edwards, L. (2011). *Role and Responsibility of Internet Intermediaries in the Field of Copyright and related rights*. Retrieved March, 26th, 2012 at http://www.wipo.int/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf. In the following the ISSP and ISP terminology will be used interchangeably.

5 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, p. 1–16.

sed on the basis of the object of their contract with the final user: if the object is the possibility to connect the user to the Internet via a telecommunication line or link, the ISP can be defined as *access* provider; if the object of the contract is the hosting of a customer's web site on ISP's technical facilities and to connect the web site with the internet, the ISPs fall in the category of *hosting* providers; finally, if the object of the contract is the supply with services regarding content (such as databases, entertainment or information offers, or online shopping, etc.) the ISP can be defined as *content* providers. Thus, the boundary between content provider, and hosting and access providers, is that access providers do not offer own content on their platform, yet they can provide third party's content. However, the evolution of web 2.0 makes this distinction no more fit for the purpose as many ISPs provide multiple services at the same time, pursuant to these definitions. Thus, the boundary between hosting provider and content provider blurs.

The above-mentioned distinction is relevant from the legal point of view as the liability regime currently applicable to ISPs was built up on such distinction. In Europe, the basic reference is the E-Commerce Directive 2000/31/EC that provided for the framework on ISP's liabilities.[6] The directive distinguished among the possible services by ISP, classifying them under the heading of 'mere conduit', 'caching' and 'hosting', providing for an exclusion of liability for these types of providers in case of infringing content available on their platforms. In particular, Art 14 provided that hosting providers are exempted from liability as long as

- they do not have actual knowledge that the material is infringing,
- they are not aware of facts or circumstances from which infringing activity is apparent, and
- upon obtaining such knowledge or awareness, they act expeditiously to remove, or to disable access to the information.

However, the directive watered down this general exemption as it adds in Art 14 (3) that the limitation of liability set out in (1) «*shall not affect the possibility for a court or authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement*».[7] Moreover, Art 15 of the directive requires that information providers are charged neither by a general monitoring obligation concerning the information they diffuse or host, nor by a general obligation to search for facts and circumstances that reveal illegal activities.

---

6 Articles 12-14 of the Directive was conceived as setting down the basis for a horizontal liability regime, applying to whatever the nature of the interests violated by the defendant is. Then, the liability test should be applied in any type of tort, whether it refers to defamation or more frequently copyright or trademark infringements.

7 Edwards clarifies that «*such 'duties of care' mean those imposed by criminal or public law e.g. aid in investigation of crime or security matters, not as extending to duties under private law, e.g., to help prevent copyright infringement - since that would negate the point of Article 15 and indeed Art 14 generally*». Edwards, L. (2011). *Role and Responsibility of Internet Intermediaries*, cit., p. 10.

Although the directive provided for a common ground, the French and Italian implementation in the national legal framework slightly differ.[8] The national legislation implementing Artt 12-15 of the E-commerce directive, are respectively Artt 6 and 9 of the Loi 2004-575 *pour la confiance dans l'économie numérique*[9] (hereinafter LCEN), and Artt 14-17 of the decreto legislativo n. 70, 9th April 2003 implementing directive 2000/31/EC (hereinafter dlgs 70/2003).[10]

Looking at the content of national rules, the distinction among mere conduit, caching and hosting was kept in both cases,[11] but where the Italian legislator copy-pasted the European text in the national legal framework,[12] the French one introduced additional features. The French text provided for an optional notification procedure,[13] in order to assess the actual knowledge of the hosting provider about allegedly infringing content stored on its platform (Art 6.I.5 LCEN): the procedure requires the claimant to provide the following elements to the hosting provider in order to make it aware of the infringement: date, details of the legal or natural person making the notification and of its recipient, description of the disputed facts with their exact location, reasons for which the content must be removed and copy of the letter sent to the content's author or editor requesting him to stop the illegal activity.[14]

Another difference, that has consequences in courts gap-filling activity, is the definition provided in the two statutory acts regarding the way in which the ISP becomes aware of the infringing material: in Art 6.I.5. LCEN, a presumption of knowledge concerning the unlawful materials arises only as a result of a «qualified» communication; whereas Art. 16 (b) of dlgs 70/2003 provides that ISP is presumably unaware of any unlawful information transmitted through its services until it receives a «*communication from the competent authorities*.»[15] Thus, where the French legislator relies on the enactment of the provided no-

8 Crabit claimed that the directive is neither full nor minimum harmonisation but a combination of the two, affirming that as regards the ISP liability the rules were set the lowest common denominator. Crabit, E. (2000). La directive sur le commerce électronique. *Revue du Droit de l'Union Européenne*, 4, 749- 833.

9 Loi n° 2004-575, 21 June 2004, JORF n° 143, 22 June 2004, p.11168

10 G.U. 14.04.2003 S. O. n. 61.

11 See Art 6.I.1 LCEN on mere conduit, Art 9 LCEN (incoporated in L. 32.3.4 Code de Poste et Communication éléctronicque) on caching, and Art 6.I.2 LCEN on hosting in the French case. Art 14 on mere conduit, Art 15 on caching and Art 16 on hosting in the Italian case.

12 Zeno-Zencovich, V. (2003). Note critiche sulla nuova disciplina del commercio elettronico dettata dal d.lgs. 70/03. *Dir. informazione e informatica*, 3, 505-519.

13 See below for the implementation of such notification procedure.

14 The *combinato disposto* of Art. 6.I.5 and Artt 6.I.2 and 6.I.3 LCEN has been defined as the French notice and takedown procedure, see van Eijk, N.A.N.M., van Engers, T.M., Wiersma, C., Jasserand, C.A. and Abel, W. (2010). Moving Towards Balance - A study into duties of care on the Internet. Retrieved March, 26th, 2012 at http://ssrn.com/abstract=1788466.

15 See that the original wording of Art 14 of the E-commerce directive did not provide any detail concerning the manner in which that knowledge could be achieved: if it could be possible through a com-

tice and take down procedure by any ISP, without involving any evaluation of the legal basis of the claims by judges or legal expert; the Italian one requires a specific intervention of the judges issuing an injunction.

From the brief description above, it is clear that, although having slight differences, the two legislative frameworks share the main basic categories defining the role and the obligations of ISP. Instead, the jurisprudence of French and Italian courts show different approaches towards similar conflicts, as it will be shown in the next section.

3. IN SEARCH OF A COMMON INTERPRETATION: THE JURISPRUDENCE OF FRENCH AND ITALIAN COURTS ON THE CONFLICTS BETWEEN CONTENT PRODUCERS AND INTERMEDIARIES

3.1. France

French caselaw developed a rich jurisprudence regarding the liability of internet intermediaries *vis-á-vis* content producers,[16] yet showing different role played by the distinction between hosting providers and 'publishers'.[17]

The most interesting cases are those decided by the Court of Appeal of Paris regarding four videos available on the online video-sharing platform Youtube.[18] In all the cases, the unauthorized copy of the content was uploaded by a user of the platform; as soon as the copyright holders found it out, sent a notice to the ISP asking for the removal of the content. Given that after a while the content was again available on the platform, the copyright holders sued the intermediary for copyright infringement. If the lower court decisions acknowledged the position of the ISP as an hosting provider, thus exonerated from liability pursuant art 6.I.2 LCEN; the same outcome was not achieved in the appeal decision. As a matter of fact, the Court of appeal addressed two issues: on the one hand, the obligation of the ISP to remove the notified videos and to prevent subsequent upload of the same videos;

---

munication from any third party, or only by a qualified source. See more on this point in Casarosa, F. (2009). Wikipedia: Exemption From Liability in Case of Immediate Removal of Unlawful Materials. *SCRIPTed*, 6, 669-676.

16 See Pointer, N. (2008). Synthèse de la jurisprudence relative à la responsabilité des plateformes communautaires non commerciales. Retrieved March, 26th, 2012 at http://www.juriscom.net/pro/visu.php?ID=1101; and also Thoumyre, L. (2010). Hyperdossier - La responsabilité des acteurs du web 2.0 entre 2006 et 2010. Retrieved March, 26th, 2012 at http://www.juriscom.net/pro/visu.php?ID=1144.

17 Stalla-Bourdillon, S. (2010). *Responsabilité civile et stratégie de régulation : essai sur la responsabilité civile des prestataires intermédiaires de service en ligne*. EUI Ph.D.Thesis. Florence: European University Institute; Stalla-Bourdillon, S. (2012). Sometimes one is not enough! Securing freedom of expression, encouraging private regulation, or subsidizing internet intermediaries or all three at the same time: the dilemma of internet intermediaries' liability. In Kierkegaard, S. and Grosheide, W. (eds.). *Copyright Law in the Making- European and Chinese Perspectives.* Co-Reach, 95-122.

18 Cour d'appel de Paris Pôle 5, Google Inc. v. Bac Films, The Factory, 14 January 2011.

and on the other, the role of the ISP as hosting provider on the basis of the features available by its search engine function.

Under the first perspective, the court ruled that ISP did correctly remove the copyright infringing materials as soon as it received the notice from the claimants, complying with the procedure provided by Art 6.I.5 LCEN. However, the exemption from liability provided by Art 6.I.7 LCEN does not apply for the subsequent upload of the infringing content as the claimants do not have the obligation to have a new notice for the same content. This implies that the ISP could be charged of a monitoring role in the case of availability of the same content, given that it holds the technical means to verify the upload through keywords, screen-shot correlation, etc. The court clarifies that this is not conflicting with the provision of Art 6.I.2 LCEN, as it does not provide for a general monitoring function of content uploaded on the video-sharing platform; instead, it requires the ISP to verify the new publication online of the specific content already notified.

Under the second perspective, the analysis of the court regarding the role of the ISP was very detailed and addressed all the criteria that could imply an intervention of the ISP in the content uploaded by users, in order to qualify the ISP as a publisher or a hosting provider. The court listed as items:

- the provision by the ISP of technical system to access the uploaded content (e.g. video on demand services, media players, etc.);
- the provision by the ISP of a search engine service allowing for indexing uploaded content;
- the terms and conditions regarding the license agreement towards the ISP; and,
- the provision of an advertising system applied to all content available.

The analysis of the court resulted in the qualification of the ISP as a hosting provider, as all the listed criteria did not prove, in the eyes of the court, the intervention over the content hosted on the platform. However, the court introduced a further element regarding the availability within the search engine function of additional links towards different platforms where the infringing content was available. In doing so, the ISP moved beyond the neutral function that characterises the hosting provider, as it did not propose the content posted by its own users, but it «*implemented an active function that, adding links, allowed it to download the content from third party sites making it available on their own pages for their users*», thus, such reference system exceed from the hosting activity.

It should be underlined that the decision of the Appeal court is not the first addressing the problem of an additional duty of care towards hosting providers, so as to impose them a monitoring activity of eventual subsequent infringements of already identified infringing material. As a matter of fact, other previous lower courts have addressed and solved in the affirmative way the question.[19] However, the one described is the first upper

19 TGI Paris, Zadig Productions v. Google Video, 19 October 2007; TGI Paris, Ordonnance de référé, Roland Madgane et al. v. YouTube, 5 March 2009 ; TGI Paris, 10 April 2009, Zadig Productions v. Dailymotion. In particular, in the most recent TGI Creteil, INA v Youtube, 14 December 2010, the court rejected the reasoning of the defendant, affirming the practical impossibility to exercise a

court that acknowledged this duty of surveillance, though the LCEN does not impose such obligation.[20]

This trend towards an increased charge of control towards ISP is confirmed also by another recent decision by the TGI, which introduced an additional element clarifying the balance between ISP and copyright holders regarding the respective role and responsibilities.[21] The case concerned a claim by a collective society holding the copyright of a set of videos against a video-sharing platform, due to the fact that the ISP did not remove all the infringing content from its platform though it received a complete notice by the claimant. The Paris Tribunal acknowledged that a video-sharing platform is obliged to react expeditiously as soon as it receive the communication of infringing content available on its hosting platform. Moreover, if the ISP holds the technical means to detect the upload of the already notified infringing content, then the copyright holder is not required to send a new notice concerning the same content. However, in this case the claimant is not exonerated from any activity after the submission of the notice, rather it should collaborate with the ISP in order to detect infringing content. If such collaboration lacks, then the ISP is not to be held liable for the case of infringing content that is subsequently made available on its platform.

The qualification of hosting provider is also debated in jurisprudence. As recent decisions show, the criteria to draw the boundary between hosting providers and publishers are still not clear, and the most controversial one is the for-profit feature of the platform, being it interpreted as a symptom of an exceeding level of interference over content or as a non pertinent element. The French Supreme Court has already addressed this issue twice, and the most recent decision reversed the approach taken in the previous decision, as it clarifies that the sale of advertising space by the website does not imply the interference by the ISP in terms of editing the content posted.[22] The reasoning of the Supreme Court confirmed lower and appeal court decisions, which emphasised that «*the LCEN provides that the hosting service can be assured even for free, in which case it is necessarily financed by advertising revenues*

monitoring over all the content uploaded by users, and the complementary claim that it did not the adequate technical means to delete the infringing copyright materials. As a matter of fact the court acknowledged that the ISP was able to delete or make inaccessible harmful or hatred content, thus the same technical tools could be used for copyright infringing content. The court, moreover, requires the ISP to adopt atechnical device to monitor and filter content, allowing also the claimant to access and verify the ffunctioning of such a device.

20 van Eijk, N.A.N.M., et al. (2010). Moving Towards Balance - A study into duties of care on the Internet cit., p. 112. It should be underlined that also the Conseil Constitutionnel intervened in reducing the leeway for court interpretation as it provided that liability for not having removed content reported as unlawful arises only when (a) the content is manifestly unlawful or (b) its removal has been ordered by a court. Otherwise, the constitutional court allocate on hosting providers the task of judging the «manifestly unlawful» nature of content and not the legality or illegality of content. See Conseil Constitionnel, décision n°2004-496 DC, 22 juin 2004.

21 TGI Paris, Sppf v. Youtube, Google France, Google Ireland, 28 April 2011.

22 Cour de Cassation, Télécom Italia (Tiscali) v. Dargaud Lombard, Lucky Comics, 14 January 2010; Cour de Cassation, Nord-Ouest Production et al. v. Dailymotion, 17 February 2011.

and that it enacts, no prohibition in principle to the commercial exploitation of a host service through advertising». Moreover, the Appeal court pointed out «*that is not demonstrated in this case, a relation between the means of remuneration by advertising and the selection of the uploaded content, as only the homepage and the standard video display have advertising space, whereas no advertising is included in users' personal pages*». Neither could the other elements listed by the claimant be invoked to attribute editorial control to the ISP: the re-codification of the video content in order to ensure the compatibility of the latter to the media display interface, or the formatting of the content in order to comply with the maximum amount of space for each file imposed by the ISP. Both previous elements are clearly involved in the technical activity provider by the ISP in order to improve the provision of the service, and none of them implies a selection of the content to be distributed through the online platform. The availability of content classification and of display presentation tools are also consistent with the hosting provider position as they are aimed at improve organisation and ease access to content for the final user, again without implying any control over the selection of the content.

3.2. Italy

In the last two years Italian courts had a few occasions to address the problem of content distribution online under different perspectives and with different results. The set of cases see the conflict between content producers, such as traditional broadcasters or film majors, opposing to search engines, either making available directly through their websites, or indirectly through links to infringing copyright materials. The decisions of the courts differ among them, in particular when defining the role of search engines vis-à-vis hosted content, and regarding filtering obligations flowing from the notice and take down procedure.

One very recent case addressed the liability of ISP for linking activity. Given the different approaches of lower and Appeal courts, it is interesting to look more deeply at the content of the two decisions. The brief description of the facts is the following, an Italian official distributor of a foreign movie sued a search engine for copyright infringement, as it made available within their search results' lists – using the title of the movie as keyword – not only the official website, but also other links where the movie would be illegally downloadable.[23]

The lower court acknowled ged the liability of the ISP and issued an injuction imposing the ISP to avoid «*continued or repeated copyright infringment of the film, by connecting via search engine indexing to websites that make fully or partly available the movie, except for the official movie website*». Two were the underlining assumptions: first, the injunction implicitly excluded that any link, except for the official movie website, could be lawful, as none of the parties opposed on this point during the discussion phase; secondly, the judge assumed that the search engine was liable as it had not reacted immediately, after the notice received by the claimant.

23 Tribunal of Rome (special section on intellectual property), PFA Films s.r.l. v. Yahoo, 22 March 2011.

Under the first perspective, the reasoning did not take into account that not all the linked websites provided for unlawful materials, given that no proof has been given by the claimant. The search engine in this case was only a third party with no interest nor knowledge about the content it indexed; thus, it could have not opposed to the claimant position.

Under the second perspective, as a consequence of the previous one, the notice received by the ISP, though formally correct, should have included a detailed specification of each of the uniform resource locator (*url*) that unlawfully provide for copyright-protected content, otherwise the mere claim by a copyright holder could trigger the deletion of all the alleged infringing websites from search results in any search engine, including also those that for instance only mention or review the copyright content. Where such level of specificity is lacking, no liability can be charged on the search engine, which indexed among hundreds of page some that provide for unlawful content. It should be underlined that the judge prohibited the search engine also to keep within the result list those links that did not redirect to the official website of the film. This implicitly imposed a filtering obligation on the search engine to verify all the indexed results excluding those that – in the view of the search engine, and not of a judge – seemed unlawfully providing copyright-protected material.

The Appeal decision, then reversed the lower court's decision,[24] solving both the issue of the content of the notice and the issue of the allocation of the burden of proof regarding infringing behaviour. First, the court required that the content of the notice sent to the ISP in order to start the take down procedure should have provided for a high level of detail, listing all the *url* where copyright infringing material could be available, rather than having a simple description of the type of content available. Moreover, the court addressed the burden of proof regarding the copyright infringment: following rule of law principles, the copyright holder should not only have proven its rights, but also the existence of breaches of third parties when asking to take down such websites. This was justified under two perspective, on the one hand, the effects of the injunction towards the intermediary would not lay only on it, but also on overall internet users community; thus, it should be sufficiently grounded, in particular when the original uploader is not convened in court. On the other hand, the level of fragmentation of distribution rights could lead to difficulties in ascertain if the conduct could truly fall in an unlawfull distribution of the content.

A different set of cases addressed the criteria upon which hosting position could be defined, in particular when ISPs are involved in the provision of different services, from simple search engine to user generated content platforms. The decisions of the courts resulted in different outcomes, though they showed a common trend.

In two decisions, [25] the Court of Milan ruled against the ISPs for copyright infringement, expressly proposing a brand new distinction within the classification provided by law, namely between active and passive hosting activity. In both cases, a broadcasting content

24 Tribunal of Rome, Yahoo v. PFA Films s.r.l., 11 July 2011.

25 Tribunal of Milan, RTI s.p.a. v. Italia On Line, 7 June 2011 and Tribunal of Milan, RTI s.p.a. v. Yahoo!, 9 September 2011.

producer claimed that several videos of its broadcast programmes were uploaded on the defendants' websites – providing for video-sharing platforms – without the company's consent. Given that the notice regarding the copyright protected materials sent to the defendants received no answer, the copyright holder brought the cases in front of a judge. The court of Milan held that the liability exemptions for hosting providers under dlgs 70/2003 did not apply to the ISPs in question, as they both had played an active role in organising the service and the videos uploaded to its website, offering additional services with a view to commercial benefit. In order to clarify the role of the ISPs, the court 'created' a distinction between 'active' and 'passive' hosting activity,[26] claiming that the recent technological evolution led to the existence of a new category of ISPs, i.e. hosting providers which do not fit with the meaning of Recital 42 of the E-Commerce Directive.[27] In the reasoning of the court, neither of the defendants could claim to act only as an intermediary in a mere «*technical, automatic and passive*» role, as they both performed the following activities:

- they provided for a system that allowed the publication of advertising links related to the videos in the view of commercial benefit;
- they provided a search engine service allowing the indexing of the uploaded videos and their contents, amplifying their visibility;
- they provide for a 'report an abuse' button that allows a peer monitoring activity; and
- the user terms and conditions of the websites included a licence agreement, according to which users grant the platforms *inter alia* the right to display, edit, adapt, modify and use the uploaded videos.

The previous items, in the judges' reasoning, showed a minimum level of editorial control, or better of 'content management' that excluded the applicability of liability exemptions provided by law. However, the criteria are over-inclusive: first, no legal provision include the commercial benefit in the elements to verify the active role of the web platform.[28] Secondly, neither the indexing nor the technical surveillance system adopted to monitor unlawful conduct could differentiate between active and passive hosting activity, given that they can be both provided automatically in order to make «*the transmission more efficient*», as long as they do not imply a control

26 Tribunal of Roma, Vividown v. Google, 15 December 2009

27 The text provides that «*the exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored*».

28 See also ECJ Case C-324/09, L'Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L'Oréal (UK) Ltd v eBay International AG, eBay Europe SARL, eBay (UK) Ltd, et al., 12 July 2011. The ECJ clearly affirmed that «*the mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability provided for by Directive 2000/31*» (par. 115).

over content.[29] Otherwise, following the judge reasoning, only a pure storage website could be defined as hosting service. Finally, though the terms and conditions include the right to modify, edit, and adapt the uploaded content, in theory, implying a level of control and intervention over content; the judges should have verified if they were exercised in practice, which was not the case.

Other two lower courts decisions[30] relied on a similar reasoning, distinguishing between passive and active hosting providers. The different outcome of the Court of Rome was due to the fact that here the claims were against two ISPs that were pure hosting providers, which offered several services to be run on their servers. Yet, video-sharing services were managed by two other companies. The distinction between active and passive hosting providers were not expressly referred to, but was applied in practice: the ISPs providing for the server storage space were not held liable for the copyright infringing material available on their servers, being only *passive* hosting providers; whereas the same exemption of liability was not applicable to the hosting providers managing the video-sharing platforms. It should be noted that the same criteria listed above by the Court of Milan were used to qualify the 'active' role of the hosting platform.

Under a different perspective, the Court of Rome confirmed the need for a sufficient level of detail in the notice regarding the copyright infringing content, as it required that it should be a formal notice sent by the rights-owners including «*detailed and specific instructions in order to remove the videos and the related web pages*». Furthermore, the Court of Rome stated that judges are not entitled to order ISPs to «*exercise a preventive control over any and all contents on the websites that are hosted on their servers*». Thus, ISPs providing hosting services cannot be requested by the courts to prevent publication of similar contents to those originally reported because such a measure would be a general monitoring obligation, prohibited by art 17 dlgs 70/2003.

4. COMPARATIVE ANALYSIS

The description of the previous cases in France and Italy, though limited to the very recent jurisprudence decided in the two countries, shows a different approach in addressing similar legal issues. The main elements that will be compared in the following are the characteristics of the notice that should be received by the ISP clarifying the users claims over infringing content available online; the obligation to monitor that is imposed to ISP, in particular as *ex ante* filtering activity; and, finally the internal distinction drawn within the hosting provider category.

29 Moreover, they could be also interpreted as an effect of the regime adopted at European level, as clarified by recital 40 of the E-commerce directive which provides that «*the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC*».

30 Tribunal of Rome, RTI s.p.a. v Choopa, 20 October 2011; Tribunal of Rome, RTI s.p.a. v Worldstream, 26 October 2011.

4.1. The content of the notice

Both French and Italian judges addressed the content of the notice that should be sent by any claimant to the ISP in order to acknowledge the presence of infringing materials on the platform of the ISP, and thus triggering its reaction so as to expeditiously delete or take down such material. The background difference between the two approach is the legislative framework that in the French case provides, as said above, a specific set of items to be included in the notice, which allow the ISP to identify easily both the infringing content and the correctness of the claim.[31]

The same level of detail is not found in the Italian legislation, where the definition of the items to be included in the notice has not been addressed. In fact, Italian court filled the gap of legislation clarifying that the information to be provided by the claimant should as precise as possible, including not only a general reference to the content that is allegedly infringing but also providing a precise list of the url where such content could be found. The same level of detail has been required also where the court acknowledged that the ISP itself could have used its technological tools (e.g. video recognition, or simple search tools) to find out the same list of results.

The detailed information to be included in the notice is an important element to strike the balance between the obligations that charge the ISP vis-à-vis the copyright holder. The French and Italian courts acknowledge that it is not reasonable to ask the ISP to take down any material that is generally claimed to be infringing copyright as it would impose an excessive burden of ISP, having also as a consequence to require the ISP to verify the prevalence of claimants rights over those of third parties, which made the infringing content available.[32] This approach could also help in solving a related issue that the neither French nor Italian legislation addressed, namely the potential liability of the ISP towards the user that has his/her content wrongly taken down.[33] In this case the completeness of the claim and, in the Italian case, the intervention of the court, could provide a defence for the ISP for the take down procedure.

---

31 See that the court had in earlier decisions affirmed that the claimant should prove the property rights over the content that he claims to have been breached, (TGI Paris, Dailymotion v. Lafesse, 18 December 2007) ; and if the ISP, though receiving a notice complying with Art 6.I.5. LCEN is allow to refuse to take down the material where it evaluates that this is not manifestly illegal (TGI Paris, Dailymotion v. Lafesse, 15 April 2008).

32 It should be noted that the ECJ introduced an additional criteria for courts to evaluate whether knowledge of the ISP can be assumed, namely also when notification of allegedly illegal activities or information «*may turn out to be insufficiently precise or inadequately substantiated, the fact remains that such notification represents, as a general rule, a factor of which the national court must take account when determining, in the light of the information so transmitted to the operator, whether the latter was actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality*» (ECJ, L'Oréal v eBay, par. 122).

33 An easier solution is provided in the US Digital Millenium Act 2000 able to improve the functioning of the liability system: if the provider, after receiving a valid notification, has removed the content uploaded by another of its clients, but the notification is subsequently rejected by the court, compensa-

4.2. The obligation to monitor

A peculiar element of the French jurisprudence is the increasing level of involvement asked to the ISP in order to provide an *ex ante* filtering activity. As the recent ECJ jurisprudence has clarified,[34] it is not possible for courts to issue an injunction where an obligation to install a system for filtering the information hosted by the ISP has the following features:

- applies to all electronic communications, both incoming and outgoing, passing via its services,
- for all its customers,
- in abstracto and as a preventive measure,
- exclusively at the expenses of the ISP, and
- for an unlimited period.[35]

In particular, the ECJ acknoledged that national courts should strike a fair balance between the protection of the intellectual property right enjoyed by copyright holders and the protection of the fundamental rights of individuals who are affected by such measures, i.a. the freedom to conduct a business enjoyed by operators such as ISPs.[36] Only when this balance is fairly struck by courts, then an additional monitoring activity towards the ISP could be imposed.

This is the approach that the French courts adopted – initially not so explicitly – in order to justify the obligation for ISPs to exercise a monitoring activity over content available on their platforms, as long as an initial notice regarding specific infringing content has been sent by the copyright holder. This was also based on the fact that ISPs already hold technical tools that allow them to filter content that is manifestly illicit (e.g. pornographic materials), thus the same tools could be applied for copyright content.[37] Moreover, the courts acknowledge

---

tion for the damages suffered by the client will be charged to the user who wrongly notified and not to the provider. See N. Elkin-Koren, «Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic», (2006) 9 *New York University Journal of Legislation and Public Policy* 15-73.

34 ECJ C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), 24 November 2011; and ECJ C- 360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM) v Netlog NV, 16 February 2012.

35 ECJ, SABAM v Netlog, par. 26. See that the ECJ had already addressed the problem of balancing copyright protection with fundamental rights, in the Promusicae case (ECJ, C-275/06, Promusicae v. Telefónica, 29 January 2008), deciding that it cannot be derived from European legislation that Member States are obliged to install a duty to provide personal data in the context of a civil procedure to ensure the effective protection of copyright, but at that time it did not provide guidelines on how the balance should be made. See F. Coudert and E. Werkers (2008), In The Aftermath of the Promusicae Case: How to Strike the Balance?, *International Journal of Law and Information Technology*, Vol. 18 No. 1, p. 51.

36 ECJ, Scarlet v SABAM, par. 45-46.

37 See the recent approach of the German courts in Higher Regional Court of Hamburg, GEMA v Rapidshare, 14 March 2012 and Regional Court of Hamburg, GEMA v Youtube, 20 April 2012.

that a balance between the obligations of the ISP and the copyright holder should be achieved, requiring the latter to collaborate with the ISP in order to prevent further infrigements.

Italian courts, instead, denied any possibility of preventive filtering activity, also in those cases where technical tools could help in finding infringing content and eventually detecting further infringements. As a matter of fact, the courts interpret also those selected filtering activity as been characterised by generality.

4.3. The distinction between active and passive host

In the light of the developments of Internet activity, the definition of hosting provider provided by the E-commerce directive is no more fit to the reality of ISPs' service provision, at least in the eyes of courts. Courts struggle to identify a set of criteria that could help in distinguishing the role of pure hosting providers from those of content providers, taking into account the fact that ISPs are able to provide different services through their platforms. The distinction between active and passive host adopted by the Italian courts is a clear example of this struggle.

The French courts instead did not explicitly use such distinction, though it was put forward by the copyright holders in the most recent Supreme court decision.[38] However, the criteria that are used to verify ISP intervention over selection and distribution of content are the same that are used by Italian courts. However, it should be underlined that, except for the for-profit nature of the ISP, the criteria are differently interpreted by national courts: as a positive proof of involvement for Italian ones, whereas the opposite is taken by French ones.

It is true that drawing the boundary of active involvement of ISP in content selection is a difficult task that has been acknowledged also by the ECJ in two recent cases.[39] Yet, the court did not provide in neither of the cases any specific set of criteria that could help national courts in their decisions, leaving them the task of verifying the level of involvement of ISPs. Obviously, the ECJ was limited, on the one hand, by the difficulties in defining criteria

38 See Cour de Cassation, Nord-Ouest Production et al. v. Dailymotion, cit. Moreover, a recent report issued by two French senators on the application of the anti-counterfeiting law includes a recommendation proposing to adapt the E-commerce Directive to introduce a new category of online service provider, service publishers (*éditeurs de services*), besides the already existing categories of hosting providers and (content) publishers. A specific liability regime would apply to this new category: stricter than the one applicable to hosting providers and softer than the one applicable to publishers. The definition would not be based on technical criteria but on the economic advantage they would draw from the direct consultation of hosted materials. See Rapport d'Information of L. Béteille and R. Yung for the French Senate, 9 February 2011. Retrieved March, 26th 2012, at http://www.senat.fr/rap/r10-296/r10-296-syn.pdf.

39 See the ECJ, C-324/09, L'Oréal SA et al. v eBay International AG et al., 12 July 2011, addressing the position of an auction platform vis-à-vis counterfeited items sold by its members; and the previous case ECJ Joint cases C-236/08, C-237/08, C-238/08, Google France SARL and Google Inc. v Louis Vuitton Malletier SA, 23 March 2010, addressing the position of the search engine vis-à-vis trademark infringements by its advertising service clients.

that could be easily overcome by the technical developments; and, on the other, by a self-restrain in providing interpretative criteria that were not included in the enacted European legislation. However, the analysis of the two national jurisprudence show that guidelines on this point would improve harmonisation. Unfortunately, this was neither acknowledged by the European Commission in the conclusions drawn from the recent consultation process regarding the E-commerce directive. In fact, the Commission refrained from modifying the definition of the ISP liability rules, eventually adopting only a more uniform process of notice and take down across Member States.[40]

5. BIBLIOGRAPHY

Benkler, Y. (2006). *The Wealth of Networks : how social production transforms markets and freedom*. New Haven [Conn.] : Yale University Press.

Bonadio, E. and Santo, M. (2011). Court of Milan holds video sharing platforms liable for copyright infringement. *Journal of Intellectual Property Law & Practice*. 7(1), 14-16.

Casarosa, F. (2009). Wikipedia: Exemption From Liability in Case of Immediate Removal of Unlawful Materials. *SCRIPTed*, 6, 669-676.

Coudert, F., and Werkers, E. (2008). In The Aftermath of the Promusicae Case: How to Strike the Balance? *International Journal of Law and Information Technology*, 18 (1) 50-73.

Crabit, E. (2000). La directive sur le commerce électronique. *Revue du Droit de l'Union Européenne*, 4, 749- 833.

de Beer, J., Clemmer, C. (2009). Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries? *Jurimetrics*, 49, 375-409.

Edwards, L. (2011). *Role and Responsibility of Internet Intermediaries in the Field of Copyright and related rights*. Retrieved March, 26th, 2012 at http://www.wipo.int/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf.

Picard, R. (2011) *Digitalisation and Media Business Models*. Retrieved March, 26th, 2012 at www.mappingdigitalmedia.org.

Pointer, N. (2008). Synthèse de la jurisprudence relative à la responsabilité des plateformes communautaires non commerciales. Retrieved March, 26th, 2012 at http://www.juriscom.net/pro/visu.php?ID=1101

Riccio, G.M. (2007). Coutry Report – Italy. In A.A.V.V. (2007). *Study of the liability of Internet intermediaries*. Retrieved March, 26th, 2012 at http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/italy_12nov2007_en.pdf.

Rosati, E. (2011). Searching responsibilities for service providers: Italian courts and AGCOM find (too) many results. *Entertainment Law Review.* 22(6), 169-174.

40 Commission Communication on 'A coherent framework for building trust in the Digital Single Market for e-commerce and online services', SEC(2011) 1640.

Stalla-Bourdillon, S. (2010). *Responsabilité civile et stratégie de régulation : essai sur la responsabilité civile des prestataires intermédiaires de service en ligne*. EUI Ph.D.Thesis. Florence: European University Institute.

Stalla-Bourdillon, S. (2012). Sometimes one is not enough! Securing freedom of expression, encouraging private regulation, or subsidizing internet intermediaries or all three at the same time: the dilemma of internet intermediaries' liability. In Kierkegaard, S. and Grosheide, W. (eds.). *Copyright Law in the Making- European and Chinese Perspectives.* Co-Reach, 95-122

Thoumyre, L. (2010). Hyperdossier - La responsabilité des acteurs du web 2.0 entre 2006 et 2010. Retrieved March, 26th, 2012 at http://www.juriscom.net/pro/visu.php?ID=1144.

van Eijk, N.A.N.M., van Engers, T.M., Wiersma, C., Jasserand, C.A. and Abel, W. (2010). *Moving Towards Balance - A study into duties of care on the Internet*. Retrieved March, 26th, 2012 at http://ssrn.com/abstract=1788466.

Verbiest, T. (2007). Country Report – France. In In A.A.V.V. (2007). *Study of the liability of Internet intermediaries*. Retrieved March, 26th, 2012 at http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/france_12Nov2007_long_fr.pdf.

Zeno-Zencovich, V. (2003). Note critiche sulla nuova disciplina del commercio elettronico dettata dal d.lgs. 70/03. *Dir. informazione e informatica*, 3, 505-519.

EMULATION IS THE MOST SINCERE FORM OF FLATTERY: RETRO VIDEOGAMES, ROM DISTRIBUTION AND COPYRIGHT

Benjamin Farrand
Lecturer in Intellectual Property Law,
The University of Strathclyde

ABSTRACT: The Internet has made it possible for amateur game creators to collaborate on projects irrespective of geographical location. The success of projects such as Minecraft, and even CounterStrike, demonstrates that 'indie' developers can create entertainment products just as popular and successful as mainstream developers with huge budgets. However, many individuals instead are more interested in the old than the new – reliving past experiences through the playing of old videogames that are no longer commercially sold. Through the creation of emulators, and the ripping of ROM images (data that allows for the playing of an emulated videogame, such as Super Mario Bros. on the Super Nintendo), games with nostalgic value can be easily distributed, played and replayed. In addition, this allows for the preservation of legacy content that may otherwise be consigned to the 'dustbin of history'.

However, irrespective of the effort and ingenuity that goes into the creation of emulation software, and the effort involved in ripping ROM data to make old games playable, are these pursuits entirely legal? The purpose of this paper is to consider the compatibility of such projects with pre-existing norms of intellectual property law, comparing and contrasting the approaches of US and EU IP regimes in their handling of emulators and ROMS. The paper will analyse the issue under pre-existing legislation and with regard to relevant case law, seeking to draw conclusions on whether the existing regimes in copyright law are compatible and satisfactorily balance the right of videogame publishers to seek fair remuneration for their work with the desire by enthusiasts to preserve and relive a form of creative culture.

KEYWORDS: Copyright, Intellectual Property, ROMs, Emulator, User Generated Content, Digital Preservation.

1. INTRODUCTION

Most of the debate concerning copyright and the Internet has focused primarily on issues relating to conventional piracy, and more so on piracy and the music and movie industries. In the EU in particular, little focus has apparently been placed on videogame piracy, and even less on the issue of the distribution of 'legacy' videogames. While some authors in the US have considered the legality of videogame emulation, there appears to be little literature on this subject from European intellectual property scholars. The issue of the distribution of digital versions of old videogames for obsolete consoles poses interesting problems for copyright law – while the distribution of such content appears to be in breach of copyright, unlike with movie and music distribution, many of the titles exchanged by videogame enthusiasts are no longer commercially available, nor are physical copies easily found in second-hand markets. Furthermore, although the distribution

of digital versions of old games may be in breach of copyright, the creation of emulators, software solutions facilitating the access and use of old videogames for discontinued hardware on personal computers represents a success for ingenuity and creativity and a method of preserving cultural artefacts. However, many in the videogame industry perceive emulators to be a threat to their business model. The purpose of this article is to consider the legality of the distribution of old videogames in the form of ROM files and the use of emulators, comparing the US and EU legal regimes in order to build analogies from US law. This is due to the limited available case-law on emulation in the EU, where the legality of emulators does not appear to have been tested within the court system. The article will also attempt to determine the impact of emulation of legacy content on the videogame industry, and whether the benefits of preservation may potentially outweigh any found detriments to copyright holders. The article will then conclude with some consideration of possible legal responses to the issue of emulation, and what policies the videogame industry may be advised to adopt.

2. EMULATORS AND ROMS: THE LEGALITIES OF RE-ENGINEERING VIDEOGAME PAST

In order to be able to effectively discuss the copyright issues that arise in the use of emulators and ROM files, it is necessary to explain the terminology and how the technology works. An emulator, or more accurately, a videogame emulator (which should not be confused with a terminal emulator), *'is a piece of hardware/software that allows a user to execute game software on a platform for which the software was not originally intended'*[1]. Or, as another source puts it, *'an emulator makes one system imitate another by tricking software into running on a computer for which it wasn't designed'*[2]. With regard to a PC (or Mac) based software emulator, the emulator program creates a virtual representation of the videogame console on the user's desktop. For example, through the use of GENS, a Sega Megadrive emulator, the user can run Sega Megadrive games on their computer, mimicking perfectly (or close to perfectly) the specifications of that videogame console. The virtual console runs as any other standard program. However, the program is the same as a console – unless you have games to play it on, it is just an empty system. Once again using the Sega Megadrive as an example, games for the system came on 16-megabit cartridges that connected to the hardware using a pin-connector system. The console itself contained no hard-disk, meaning that if the console were switched on without a game cartridge inserted, the user would be presented with

1 Conley, J., Andros, E., Chinai, P., Lipkowitz, E. & Perez, E. [2004] *'Use of a Game Over: - Emulation and the Videogame Industry, a White Paper'*, Northwestern Journal of Technology and Intellectual Property 2(2) 261 at p.264

2 O'Brien, T. (09/04/2011) *'Switched's Comprehensive Guide to Videogame Emulators',* Switched. Retrieved on 25th February 2011 from http://www.switched.com/video-game-emulators/switched-ultimate-guide-retro-gaming/

a blank screen on the TV that the system was connected to. Without game information loaded into the emulator program, the user will also be presented with a blank screen. The videogame itself is stored on the videogame cartridge as Read Only Memory, known by the acronym ROM. For use with a videogame emulator, the ROM data on the cartridge is extracted (also known as 'ripping'), and dumped into a 'ROM' file. For this reason, the files that contain code for videogames are known as ROMs.

2.1. A *prima facie* case of infringement? Copyright and videogame emulation

On first viewing, it would appear that the use of emulators and ROMs would be a standard case of copyright infringement. Through the use of emulation software combined with a ROM file, a user can avoid paying for a videogame, and instead download a copy of that game from the Internet. Corporations such as Nintendo argue this in strong terms; *'the introduction of emulators created to play illegal software represents the greatest threat to date to the intellectual property rights of video game developers…such emulators have the potential to significantly damage a worldwide entertainment software industry*[3]. The Entertainment Software Association (ESA) argues that it is *'illegal to make or distribute software or hardware emulators or ROMs without the copyright or trademark owners' permission*[4]. In order to assess whether this is true, however, and to determine the extent to which ROMs and emulators are illegal, it is necessary to separate the two types of software and consider them on their own merits.

The first item for consideration is the ROM. In the EU, computer programs are granted copyright protection under Article 1 of the Software Directive[5], which states that *'Member States shall protect computer programs, by copyright, as literary works…protection in accordance with this Directive shall apply to the expression in any form of a computer program. Ideas and principles which underlie any element of a computer program…are not protected*[6]. Whereas in the UK the protection of computer programs as literary works predates the Software Directive[7], other countries such as Spain and France granted protection as lite-

3 Nintendo Corporate, *'Legal Information (Copyrights, Emulators, ROMs, etc.)'*, (original date of creation not stated, last modified 28/04/2012) retrieved on 25th February 2012 from http://www.nintendo.com/corp/legal.jsp

4 ESA, *'Anti-Piracy Frequently Asked Questions'*, ESA Policy, (original date of creation not stated, last modified 28/04/2012) retrieved on 25th February 2012 from http://www.theesa.com/policy/antipiracy_faq.asp#6

5 Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version), replacing Council Directive 91/250/EEC of 14 May 1991

6 Software Directive, Article1(1) and Article 1(2)

7 Copyright, Designs and Patents Act 1988, c.48, s.3(1)(b), although it was originally stated that computer programs could be covered by copyright as literary works in the UK as far back as 1977, according to the *Whitford Report*, Report of the Commission to Consider the Law on Copyright and Designs 17 (Cmnd. 6732 H.M.S.O. Mar. 1977)

rary works through the implementation of the Directive in national legislation[8]. Although the Directive does not explicitly define computer programs, and indeed the Commission has stated a hesitance to use an explicit definition on the grounds that any definition may become outdated by developments in technology[9], this lack of an explicit definition does not appear to have caused significant problems in the protection of computer programs as literary works in the European Union[10]. In comparison, the US has specifically defined a 'computer program' as being *'a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result'*[11]. Videogames form an interesting case study for the analysis of copyright as applicable to computer programs, as Professor Irini Stamatoudi has commented upon in significant detail[12]. Initially, the treatment of videogames as copyrighted works was initially far from certain, with individual nations treating them dissimilarly[13]. At least one explanation for this, reasons Professor Stamatoudi, is that *'videogames were new to the market. Their commercial value was not immediately evident and neither was their need for protection'*[14]. For example, in the US during the early 1980s, videogames were deemed not to be subject to copyright protection. In the case of *Atari v Phillips*[15], which concerned a possible infringement of copyright regarding the game Pac-Man, it was determined that computer games were not protected by copyright, as they amounted to little more than systems or procedures, which were specifically excluded from copyright protection[16].

Nevertheless, elements of the game may be copyrightable as an audiovisual work – despite their being no protection of the game as a work in itself, *'the audio component and the concrete details of the visual presentation constitute the copyrightable expression of that game*

8 Ley 16/1993, de 23 de diciembre de incorporación al Derecho español de la Directiva 91/250/CEE, de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador Art 1(1) and Loi n° 94-361 du 10 mai 1994 portant mise en oeuvre de la directive (C. E. E.) n° 91-250 du Conseil des communautés européennes en date du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur et modifiant le code de la propriété intellectuelle Art 1 respectively.

9 COMMISSION STAFF WORKING PAPER on the review of the EC legal framework in the field of copyright and related rights, SEC(2004) 995, Brussels (19/07/2004) at para. 2.2.1.1

10 Commission of the European Communities, 'Report from the Commission to the Council, the European Parliament and the Economic and Social Committee on the implementation and effects of Directive 91/250/EEC on the legal protection of computer programs, COM(2000) 199 final (10/04/2000) at p.20

11 17 USC §101

12 See Stamatoudi, I. (2007) *'Copyright and Multimedia Products: - A Comparative Analysis'*, Cambridge University Press pp.166-185

13 *Ibid* at pp.167-168

14 *Ibid* at p.168

15 *Atari v North American Phillips Consumer Electronics Corp* 672 F.2d (7th Cir. 1982)

16 See also Glasser, A.R. (1987) *'Video Voodoo: - Copyright in Video Game Computer Programs'*, 38 Fed. Comm. L.J. 103 at p.107

«idea»'[17]. This reasoning may be explained by the fact that earlier videogames such as Pac-Man constituted very simple procedures, such as navigating a maze, and the protection of these works in this form would be too close to the protection of an idea, rather than the expression of that idea. Therefore, if a character were too similar to Pac-Man in its artistic representation, this would constitute an infringement over the copyright of the graphical representation, whereas a game with significantly different characters navigating a maze would not be deemed significantly distinct or original, and would therefore not constitute an infringement. As games have become more complex, however, and with relatively recent legislative developments, the situation is somewhat different. As one writer commented, *'both the audiovisual display and the videogame computer program enjoy independent copyrights'*[18]. Professor Stamatoudi expands upon this, stating that videogames can *'qualify as computer programs, as audiovisual works, as a combination of the two, or where not enough originality is found to classify them as such, they can perhaps attract copyright protection as drawings for their characters, figures or other designs'*[19].

In the US, the computer program itself is protected as a literary work by virtue of its code following the case of *Apple v Franklin*[20], where the court determined that the category of literary works was not restricted to literature in the conventional sense. In addition to written literary texts such as Alice in Wonderland, the category 'literary works' in US copyright law was deemed to also cover numbers or symbols with a given meaning, concluding therefore that *'a computer program, whether in object code or source code, is a «literary work» and is protected from unauthorised copying…'*[21]. English case law pursuant to the Software Directive has adopted a similar approach. In the 2007 case *Nova Productions v Mazooma Games*[22], the English Court of Appeal determined that videogames were afforded protection both as audiovisual works and literary works, stating that infringement of copyright as regarding the videogame as a literary work would not occur where *'nothing has been taken in terms of program code or program architecture'*[23].

What does this mean for videogame ROM files? Ultimately, based on their protection both as computer programs and as audiovisual works, a copy of a ROM file constitutes the wholesale copying of the entire game, including both the source code and audiovisual representation of that code during play. This indicates that the distribution of these files by collectors on the Internet constitutes what is known as a secondary infringement of copyright. Whereas primary infringement is committed by the act of copying a creative work, such as by making a copy of the ROM file, secondary infringement applies to 'dea-

17 *Atari v Phillips supra 15* at p.617

18 Glasser, A.R. *supra 16* at p.103

19 Stamatoudi, I. *supra 12* at p.176

20 *Apple Computer, Inc v Franklin Computer Corporation* 714 F.2d 1240 (3rd Cir. 1983)

21 *Ibid* at p.1249

22 *Nova Productions Ltd v Mazooma Games Ltd & Others* [2007] EWCA Civ 219

23 *Ibid* at paragraph 30

ling in' an infringing work, such as through distribution of that infringing ROM file. The uploader of a ROM may therefore be found liable for both primary infringement through the making of a copy, in addition to secondary liability through dissemination, whereas a downloader may be found to only commit an act of primary infringement through the making of a copy through the act od downloading. To distribute these files interferes with the exclusive reproduction and making available rights of copyright holders provided for under the Information Society Directive[24] in the European Union, and the exclusive reproduction and distribution rights in the US[25]. Could it be that Nintendo's previously stated stance on ROMs and emulators is correct?

2.2. Good coders copy, great coders steal? Reverse engineering and the legality of emulators

It must be stated that the distribution of ROM files of copyrighted videogames may constitute an infringement of copyright, the legal situation regarding the creation and use of emulators is not as clear. Unfortunately (or, perhaps, fortunately for those involved in the distribution and downloading of emulators), there appears to be no case law at the European level, and little if any case law at the national level that expressly deals with copyright issues as applicable to emulators in the EU. As such, the only definitive cases involving these issues appear to originate in the United States. One of the first relevant cases is that of *Sega Enterprises v Accolade*[26], which concerned the reverse engineering of Sega code by Accolade. During the 1990s, the Sega Megadrive (known as the Sega Genesis in the US) was one of the two dominant videogame consoles (the other being Nintendo's Super Nintendo) in the US market. Sega could grant independent videogame producers a license over the copyrighted code and trademark of Sega in order to develop games for the console, which would then sell in competition with Sega-produced games. However, Accolade was not licensed to use the code or trademark, as licensing negotiations broke down with Sega. This was due to a demand by Sega that Sega would be the exclusive manufacturer of all games produced by Accolade[27]. In order to produce games for the system, Accolade employees bought a Megadrive console and three games, connected the system to a decompiler, and generated a print out of the source code for the system, a process known as 'disassembly'[28]. A decompiler, briefly, is a computer program or piece of hardware that takes an executable program and translates it into machine-readable code. They then loaded the disassembled code back into a computer, and experimented with it in order to discover the interface specifications

24 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Articles 2 and 3

25 17 USC §106(1) and (3)

26 *Sega Enterprises Ltd v Accolade Ltd,* 977 F.2d 1510 (9th Cir. 1992)

27 *Ibid* at paragraph 2

28 *Ibid* at paragraph 4

for the Genesis console by modifying the decompiled programs and studying the results[29]. This process is called 'reverse engineering'. Usually, this process is performed using the 'clean room' technique where the work is *'carried out by two different people…one person writes the specification* (after determining what exactly the decompiled code does) *and the other later codes the result, so that the coder has not seen the original code'*[30]. In this case, Accolade initially did not copy any of Sega's proprietary code, and instead wrote distinct code to achieve the same result of allowing functionality with the Sega system. However, due Sega's concerns with the possible piracy of videogame cartridges, they created a form of technical prevention for the new version of the system, known as the Genesis III. This protection was in the form of a code – the Trademark Security System (TMSS). This system was held on the console microprocessor, which would check for 4 bytes of data in the header file contained on an inserted cartridge. The data would spell the name SEGA, and if detected, the console visual output would display the message «PRODUCED BY OR UNDER LICENSE FROM SEGA ENTERPRISES LTD». If these 4 bytes were not found on the system, then the game would not run. In order to ensure Accolade games would run on the new system, Accolade inserted this line of code into the header file of the game ROM. Ultimately, Sega brought a legal action against Accolade, on the grounds of copyright and trademark infringement.

In considering the case, the Court of Appeal determined that infringement through the use of intermediary code (the code displayed through the decompiling process) may ultimately constitute fair use, *'where disassembly is the only way to gain access to the ideas and functional elements contained in a copyrighted computer program and where there is legitimate reason for seeking such access'*[31]. In reaching such a decision, the Court deemed that the use of code was related to ensuring functionality with Sega's console, specifically stating that functional requirements are not protected by US copyright under 17 USC §102(b)[32]. With regard to the trademark issue, the Court seemed particularly unimpressed with Sega's use of a trademark as a technical prevention mechanism, stating that its use did not constitute a legitimate use of trademark[33], and therefore the action by Accolade did not infringe upon Sega's intellectual property right. This right to reverse engineer code, established in the Accolade case appears to have been enshrined in the Digital Millennium Copyright Act (or DMCA), written six years after the case's conclusion, where it is stated that:

> *'a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure*[34] *that effectively controls access to a particular portion of that program for the sole purpose*

29 *Ibid*

30 Conley, J., Andros, E., Chinai, P., Lipkowitz, E. & Perez, E. *supra 1* at p.274

31 *Ibid* at paragraph 72

32 *Ibid* at paragraph 46

33 *Ibid* at paragraph 81

34 It is worth mentioning briefly at this stage the notion of a TPM. A TPM is a way of preventing the copying of a digital work, whether in the form of ROM or MP3 file, or the data on a DVD or Blu-ray disc, through the use of encryption technologies. The breaking of an encryption code, for example,

of identifying and analysing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention[35].

In addition, US case law has determined that the creation of videogame emulators constitute a legitimate goal for which the fair use protection offered to reverse engineering may be granted. This is the result of two cases, *Sony v Connectix*[36] and *Sony v Bleem*[37]. Both cases concerned the creation of videogame emulators of the Sony Playstation system, a console that took both Sega and Nintendo by surprise upon its 1994 release. The Playstation was Sony's first foray into the videogame console market, and proved to be highly successful. Whereas the competing consoles the Sega Saturn and Nintendo 64 sold 9.2 million units and 32.9 million units respectively, during its lifetime the Playstation sold over 100 million units[38]. Given its popularity, it appears almost inevitable that the console would be a source of interest to emulator communities. In the *Connectix* case, Connectix created and sold emulation software called 'Virtual Game Station'. The software did not use any of Sony's code in the final program, although code was decompiled in order to construct the emulator. In the Court's reasoning, it was determined that the correct precedent to follow was that set by the Sega case. The Court considered that the software did not merely supersede the objects of the original creation, but instead add something new, in essence, a transformative work. *'The product creates a new platform, the personal computer, on which consumers can play games designed for the Sony PlayStation…* (affording) *opportunities for game play in new environments, specifically anywhere a Sony PlayStation console and television are not available…* (it) *is a wholly new product, notwithstanding the similarity of uses and functions between the Sony PlayStation and the Virtual Game Station…* [39]. The confirmation of the legality of emulators was confirmed in the Bleem case (which in itself considered the potential breach of copyright by Bleem for showing pictures of Playstation games in its marketing, which the Court determined to be permitted comparative advertising), when it was stated that *'we have already ruled that the emulator is not a violation of the copyright laws*[40].

Although there are no cases that appear to deal with the issue of emulators in EU law, it may be inferred from the reading of the Software Directive that emulators created through

---

in order to access source-code, would constitute an act of TPM circumvention, as it allows for behaviour that the right holder wished to prevent. Digital Rights Management, or DRM, is any system of technology implemented by a right holder in order to control or limit access to a copyrighted work. Therefore, TPMs form a subset of DRMs.

35 17 USC §1201(f)(1) as created by the DMCA.

36 *Sony Computer Entertainment Inc v Connectix Corp*, 203 F.3d 596 (9th Cir. 2000)

37 *Sony Computer Entertainment Inc v Bleem LLC,* 214 F.3d 1022 (9th Cir. 2000)

38 PVC Museum (2005) *'Total Worldwide Console Hardware Sales'* retrieved on 25th February 2012 from http://www.pvcmuseum.com/games/charts/total-worldwide-console-hardware-sales.htm

39 *Sony Computer Entertainment Inc v Connectix Corp*, *supra 36* at s.3

40 *Sony Computer Entertainment Inc v Bleem LLC, supra 36* at paragraph 32

reverse engineering would also be considered legal under similar conditions. The Software Directive states at Article 6 that decompilation for the purposes of achieving interoperability of an independently created computer program with other programs will be permitted so long as it is indispensable to obtaining the information necessary to achieve that interoperability. According to Article 6(1), this will be permitted only if the decompiling is performed by someone who has a license to use a copy of the program, the information required is not already readily available, and the acts of decompilation are confined to the parts of the original program which are necessary to achieve interoperability. In addition, subsection 2 dictates that the information cannot be used for any other purpose except achieving interoperability, to be given to others, or used to create *'competing computer programs substantially similar in its expression, or for any other act which infringes copyright'*[41]. One potential problem that could be perceived as arising is that the Directive only covers software-to-software emulation, rather than hardware-to-software interoperability functions. However, there are reasons why this is unlikely. The first is that although a videogame emulator may emulate (and thus require source code from) a console, i.e. hardware, the hardware is not involved in the use of the emulator, and the only interoperability is between the software emulator installed on a computer, and the software video game. Therefore, videogame emulators appear to meet the requirement of constituting software-to-software interoperability. Furthermore, although arguments have been raised that Article 6 may be too restrictive in its scope, and that its current reading may prevent hardware-to-software interoperability software, the Working Paper nevertheless concludes that *'there is no jurisprudence to support these claims; nor is there any other evidence to suggest that there would be a need for revision'*[42]. It would appear then, that as it stands, the Directive poses no substantial bar to emulators created through the decompilation of code. With respect to the requirement that the software does not create a competing program substantially similar in its expression, it would be hoped that the European Court of Justice or national courts would take a similar view of that of the Court of Appeal in the *Sega* and *Connectix* cases; namely that the emulator only imitates the functional requirements of the console, which cannot be copyrighted, and would constitute an entirely new product, serving a different purpose than that of the original console. So long as the clean room technique is used for the decompiling of the proprietary code and the building of the new code, then it should be the case that the created emulation software is considered compliant with the Software Directive.

2.3. Emulation, preservation, termination? A consideration of the impact of ROM distribution

Despite the potential illegality of the distribution of ROMs, websites offering these files are still readily accessible on the Internet. There are however possible reasons, and indeed significant benefits, for this. The first is that it assists in the preservation of cultural

41 Software Directive Article 6(2)(c)

42 Working Paper *supra 9* at para. 2.2.1.3

products. As one article states, the business model of console manufacturers relies on *'planned obsolescence in which they introduce a new system every five years'*[43]. A short time after this, the previous console is no longer supported, and games for that console no longer sold. As one writer for Maximum PC magazine wrote, *'while the major companies are only too willing to consign older products to oblivion, hardcore game fans are busting their collective asses to keep them alive'*[44]. This may be important – as academics from the Vienna University of Technology have stated in one paper, the consignment of videogame consoles and the respective game cartridges to museums as a means of preservation does not appear to be suitable; *'console videogame systems are usually built from custom manufactured parts which cannot be replaced once broken'*[45], and the videogame cartridges become less reliable over a period of years. When dealing with cartridges with an internal battery (used for saving game data in longer games such as Role-Playing Games, for example), their ability to successfully store and restore data becomes compromised after a period of 10 years. Many games for systems from the 16-bit era, such as the Sega Genesis and Super Nintendo, are now over 20 years old. Therefore, the paper argues, *'emulation may be the most promising solution'*[46] for the long-term preservation of videogame data, with the videogames being stored as ROM files. A digital file is not subject to the same risks of damage and obsolescence as videogame cartridges, and through circulation on the Internet, videogames for 'legacy' systems may be effectively preserved for future generations to use. Nevertheless, this does not constitute a valid defence to the breach of copyright – as one paper argues, *'the preservation argument is relatively weak* (as a raised defence to infringement)*, since only copyright holders can determine whether they wish their software to be archived'*[47]. While the Information Society Directive Article 5(2)(c) allows for specific acts of reproduction by institutions such as libraries, educational institutions and museums which are not for direct or indirect economic benefit, it is difficult to argue that this restriction on copyright could be relied upon by those distributing ROM files, even if the provision was enacted in national legislation[48].

---

43 Conley, J., Andros, E., Chinai, P., Lipkowitz, E. & Perez, E. *supra 1* at pp.269-270

44 McDonald, T.L. (September 1999) *'You Will Be Emulated: - Console Emulators are Not Piracy; They're Ingenuity at Work'*, Maximum PC September 1999 at p.41

45 Guttenbrunner, M., Becker, C., Rauber, A. & Kehrberg, C. (2008) *'Evaluating Strategies for the Preservation of Console Video Games'* Association for the Advancement of Artificial Intelligence, Vienna University of Technology, at p.3

46 *Ibid* at p.3

47 Conley, J., Andros, E., Chinai, P., Lipkowitz, E. & Perez, E. *supra 1* at p.270

48 The exceptions and restrictions on copyright provided for by the Information Society Directive Article 5(2) form an optional list of exceptions that a Member State may choose to implement in national legislation. For example, many Member States implemented this section but exempted educational institutions from the section, and Ireland did not implement this section at all. See, for example, Institute for Information Law (February 2007), *'Study on the Implementation and Effect in Member States' Law of Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society'* University of Amsterdam, in particular Part II of the Report, Westkamp, G. (2007) *'The Implementation of Directive 2001/29/EC in the Member States'*, at p.22

After all, Nintendo argues that even if people claim that the use of emulators and ROMs help publishers by making old games that are no longer sold by the copyright holder available in new formats, *'it is illegal…if these vintage titles are available far and wide, it undermines the value of this intellectual property…the assumption that the games involved are vintage…is incorrect. Nintendo is famous for bringing back to life its popular characters for its newer systems…'*[49]. However, there are problems with this argument. Although it may be illegal, the second part of the argument is somewhat incoherent. Nintendo claims the titles are vintage, but then contradictorily that they're not actually vintage. Therefore ROMs (and, in Nintendo's view, emulators) should be illegal, because the distribution of otherwise inaccessible legacy content undermines the ability to make new content. Firstly, the argument that it undermines the intellectual property is questionable. As the Gower Review of intellectual property in the UK commented, *'the existence of such a large volume of old work protected but unavailable means that a great amount of intellectual capital is wasted'*[50]. The result is that the locking away of this content, which is not being commercially exploited, does not benefit society under either the US or EU systems. One economics researcher at the University of Cambridge determined that the optimal duration of copyright would be approximately 15 years[51]. This would give a creator more than enough time to recoup their costs, while allowing non-profitable works to enter the public domain. With a console and videogames that are 20 years old, and no longer exploited commercially by the creators, there is no revenue being generated through sales that can be used to subsidise the creation of new works by, for example, Nintendo.

Furthermore, it is unlikely that legacy games compete with newly released games in terms of sales. For example, it is unlikely that Super Mario Bros., a 2D-platforming game released for the Nintendo Entertainment System (NES) in 1985 effectively competes with Super Mario Galaxy, a 3D-platforming game for the Nintendo Wii released in 2007. The games are likely to cater to different audiences; as one journalist commented, *'the arcade games of the 1980s were laughably primitive compared to the immersive 3-D games we take for granted today. Who would want to play Donkey Kong when he could choose Halo or Splinter Cell instead?'*[52] According to another author, *'with hardware capacities expanding almost monthly, and computer programmers learning faster, smarter and better-looking ways to style their games, any game three months after release is considered old and outdated'*[53]. There is also nothing in the release of a ROM file that appears to prevent Nintendo from continuing to exploit the

49 Nintendo Corporate, *supra 3*

50 Gowers, A. (November 2006) *'Gowers Review of Intellectual Property'* prepared for HM Treasury, British Government, s.3.30

51 Pollock, R. (August 2007) *'Forever minus a day? Some theory and empirics of optimal copyright'*, University of Cambridge. Retrieved 27th February 2012 from http://www.rufuspollock.org/economics/papers/optimal_copyright.pdf

52 Bray, H. (2004) *'Consoles allow nostalgia buffs to play 1980s arcade favorites'*, Boston Globe

53 Dean Lord IV, J. (2005) *'Would You Like to Play Again? Saving classic videogames from virtual extinction through statutory licensing',* 35 Sw. U. L. Rev 401 at p.409

character of Mario in new games – the release of legacy games happening to feature the same character does not in any way limit Nintendo's rights over the creation of a new Mario game.

As mentioned at the beginning of this section, the business model of the videogame industry relies on planned obsolescence, and the replacement of old consoles and games with new, usually in the space of five years. Unlike the music industry, for example, the business model does not predominantly rely upon the re-releasing of old content on new media, but on continued innovation and the creation of new products. For this reason, the claim that emulation is a considerable economic threat to the videogame industry should be questioned. To provide one example, one of the previously quoted papers states that *'game enthusiasts can download 298 Nintendo 64 games along with an emulator in less than one hour, an act that results in a potential US$10,920 loss per customer to the gaming industry*[54]. This does of course assume that the average consumer would both have $10,920 to spend on Nintendo games, and the somewhat contested view that every act of downloading equals a lost sale. As one academic stated with regard to the sale of counterfeit DVDs, *"it may be that a fake DVD bought at £2 represents a lost legitimate sale at £10, but it very well may not*[55]. The article presents the yearly sales figures for Nintendo 64 software, demonstrating a fall of revenue from $1.34 billion at the peak of the console's sales in 1998, to just under $59 million in 2002[56]. Two points are worth mentioning regarding these figures – firstly, that 2002 was not only the seventh year of the Nintendo 64's life, but also the year after the console was replaced by Nintendo's 6th generation console the Nintendo Gamecube, which would help to explain such a drastic fall in sales. Secondly, the first Nintendo 64 emulator, UltraHE was released in 1999, in the fifth year of the console's lifespan. In 1999, the sales revenue for software was $1.28 billion, and in the following year, in which the Gamecube was released, $526 million. When it comes to the purchase of tens of thousands of dollars worth of videogames, the figures presented as potential losses due to videogame emulation, although potential, are highly unlikely. It also assumes that each download could be legitimately purchased – given the business model of the videogame industry, this is also difficult to argue, as it is likely that in 2002 the majority of Nintendo 64 software was removed from videogame store shelves in order to make room for sixth generation stock. To take another example, a copy of the Role-Playing Game «Sword of Vermillion» for the Sega Megadrive, for example, cannot be legitimately purchased from Sega, and the only way of legally purchasing such a game would be to attempt to find it at second-hand stores, or on online auction sites such as eBay (in addition of course, to either having or purchasing a still-functioning Sega Megadrive). Even if such a copy *were* found, the proceeds of the second-hand sale would not go to Sega. Therefore, the only feasible way to obtain the game would be to download the ROM and emulator to play it on.

---

54 Conley, J., Andros, E., Chinai, P., Lipkowitz, E. & Perez, E. *supra 1* at p.261

55 Mackenzie, S. (2010) *'Counterfeiting as corporate externality: intellectual property crime and global insecurity'* Crime Law and Social Change 54 21-38 at p.23

56 Conley, J., Andros, E., Chinai, P., Lipkowitz, E. & Perez, E. *supra 1* at p.268

3. POSSIBLE LEGAL APPROACHES TO EMULATION

There are several ways in which the issue of ROM distribution could be handled. The first would be for companies like Nintendo to try to curb the distribution of old videogames through issuing takedown requests to websites hosting these files, and issuing legal proceedings against those involved in distribution. However, such an approach would potentially have little success, and probably make little economic sense. The music industry publicly announced the end of mass lawsuits against the sharers of music files, with critics stating that the lawsuits *'did little to stem the tide of illegally downloaded music…* (and) *created a public relations disaster*[57]. The cost-effectiveness of bringing lawsuits against those sharing ROMs of games from the 1990s, for example, is highly debatable.

Indeed, the older the system, the less likely that a company is to take legal action against distributors of game content; often the games *'had been off the market so long that their manufacturers didn't care*[58]. There is little incentive to go after individuals sharing games that have been out of print for more than ten years, and such action would appear to make little commercial sense. This is in stark contrast to other creative industries – *'it would be ludicrous in any other industry to say that just because a copyrighted work was old, yet not in the public domain, that its copyright should be ignored, but that is exactly what is happening*[59]. What actions have been brought, as in the case of Sony's actions against Bleem and Connectix and Nintendo's threat of action against the creators of the UltraHE emulator, are actions based on emulation of current or almost-current emulators. The ESA, when it has brought actions against infringers, has done so primarily against those distributing ROM files for systems still being commercially sold[60]. However, as mentioned at the beginning of this article, given that the first emulators are often released four years after the release of the new console and the average lifespan of a console before the release of the next system is approximately five years, this gives the videogame industry significant time to commercially exploit those games – after the five year period, sales are likely to be minimal. It is also worth noting that as games consoles become more technically advanced, emulation becomes much more difficult. At the time of writing, it appears that there are no viable emulators for the Xbox 360 or Playstation 3, despite these consoles being released in 2005 and 2006 respectively.

The videogame industry can also benefit through the exploitation of emulation software. As games experience popular revivals, the rerelease of older games in compilation form can occur. For example, Backbone Entertainment, in partnership with Sega, has released the Sega Ultimate Megadrive Collection for the Xbox 360 and Playstation 3, which contain 40 Megadrive games run on Backbone's emulation software. The disc also contains bonus

57 McBride, S. & Smith, E. (19/12/2008) *'Music Industry to Abandon Mass Suits'*, Wall Street Journal. Retrieved 1st March 2012 from http://online.wsj.com/article/SB122966038836021137.html

58 Bray, H. *supra 52*

59 Dean Lord IV, J. *supra 53* at pp.411-412

60 *Ibid*

content such as interviews with game creators and design sketches for the games contained, providing additional value for those who decide to purchase the content. Despite the availability of these games as ROM files, a significant number of copies were sold. According to one source, in the week of the compilation's release, it was the top-selling game in the US on both the Playstation 3 and Xbox 360, beating triple-A titles such as Batman: - Arkham Asylum and Guitar Hero: - Beatles Edition[61] from Amazon sales alone. Nintendo also has a 'Virtual Console' for its Nintendo Wii, where consumers can purchase some legacy games such as the Super Mario games as downloadable content that runs on an internal software emulator.

However, the officially released Megadrive games represent 40 titles out of 915 games released for the system. In comparison, the number of Super Nintendo games released for the Wii's Virtual Console total 101 in Japan, 72 in the US, and 65 in Europe, out of a total of 784. It is unlikely that companies such as Sega and Nintendo would release their entire back catalogues through these systems, as *'with thirty-four years of history and counting, there are too many titles to reasonably expect they will all see release in the future'*[62]. In some instances, companies release old games under license, allowing games to be distributed freely, so long as it is done on a non-commercial basis[63]. Perhaps one solution for the videogame industry is to consider adopting a policy of allowing for the distribution of content publicly released more than 10 years ago (provided that the content is not for a current generation console) on discontinued systems. As the Sega Ultimate Megadrive Collection shows, the pre-existence of ROM files of games does not appear to seriously prejudice the sales of rereleased legacy content, and a non-commercial licensing may regime also result in the generation of a considerable amount of goodwill for the videogame publishers involved.

4. BIBLIOGRAPHY

European Legislation

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

---

61 Cowan, D. (18/09/2009) *'Saling the World: - Scribblenauts, Beatles Rock Band Lead US Sales'*, GamaSutra. Retrieved 02/03/2011 from http://www.gamasutra.com/php-bin/news_index.php?story=25315

62 Dean Lord IV, J. *supra 53* at p.411

63 Exidy, for example, have released 14 games they produced for arcade systems during the 1970s and 1980s for use on arcade emulators. For more information, please see the official MAME website, *'ROMs available for free download'*, retrieved 02/03/2011 from http://mamedev.org/roms/

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version), replacing Council Directive 91/250/EEC of 14 May 1991

National Legislation (chronologically)

United States Code, Title 17 – Copyright (1947) as amended (US)

Copyright, Designs and Patents Act 1988, c.48 (UK)

Ley 16/1993, de 23 de diciembre de incorporación al Derecho español de la Directiva 91/250/CEE, de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador

Loi n° 94-361 du 10 mai 1994 portant mise en oeuvre de la directive (C. E. E.) n° 91-250 du Conseil des communautés européennes en date du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur et modifiant le code de la propriété intellectuelle

Case-law (chronologically)

United States:

Atari v North American Phillips Consumer Electronics Corp 672 F.2d (7th Cir. 1982)

Apple Computer, Inc v Franklin Computer Corporation 714 F.2d 1240 (3rd Cir. 1983)

Sega Enterprises Ltd v Accolade Ltd, 977 F.2d 1510 (9th Cir. 1992)

Sony Computer Entertainment Inc v Connectix Corp, 203 F.3d 596 (9th Cir. 2000)

Sony Computer Entertainment Inc v Bleem LLC, 214 F.3d 1022 (9th Cir. 2000)

United Kingdom:

Nova Productions Ltd v Mazooma Games Ltd & Others [2007] EWCA Civ 219

Official reports (chronologically)

Whitford Report, Report of the Commission to Consider the Law on Copyright and Designs 17 (Cmnd. 6732 H.M.S.O. Mar. 1977) (UK)

Commission of the European Communities, 'Report from the Commission to the Council, the European Parliament and the Economic and Social Committee on the implementation and effects of Directive 91/250/EEC on the legal protection of computer programs, COM(2000) 199 final (10/04/2000)

COMMISSION STAFF WORKING PAPER on the review of the EC legal framework in the field of copyright and related rights, SEC(2004) 995, Brussels (19/07/2004)

Gowers, A. (November 2006) *'Gowers Review of Intellectual Property'* prepared for HM Treasury, British Government

Institute for Information Law (February 2007), *'Study on the Implementation and Effect in Member States' Law of Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society'* University of Amsterdam, in particular Part II of the Report, Westkamp, G. (2007) *'The Implementation of Directive 2001/29/EC in the Member States'*,

Press Releases and FAQs (alphabetical by author)

ESA, *'Anti-Piracy Frequently Asked Questions'*, ESA Policy, retrieved on 25th February 2012 from http://www.theesa.com/policy/antipiracy_faq.asp#6

Nintendo Corporate, *'Legal Information (Copyrights, Emulators, ROMs, etc.)'*, retrieved on 25th February 2012 from http://www.nintendo.com/corp/legal.js

Books (alphabetically by author)

Stamatoudi, I. (2007) *'Copyright and Multimedia Products: - A Comparative Analysis'* , Cambridge University Press

Articles (alphabetically by author)

Bray, H. (2004) *'Consoles allow nostalgia buffs to play 1980s arcade favorites'*, Boston Globe

Conley, J., Andros, E., Chinai, P., Lipkowitz, E. & Perez, E. [2004] *'Use of a Game Over: - Emulation and the Videogame Industry, a White Paper'*, Northwestern Journal of Technology and Intellectual Property 2(2) 261

Cowan, D. (18/09/2009) *'Saling the World: - Scribblenauts, Beatles Rock Band Lead US Sales'*, GamaSutra. Retrieved 2nd March 2012 from http://www.gamasutra.com/php-bin/news_index.php?story=25315

Dean Lord IV, J. (2005) *'Would You Like to Play Again? Saving classic videogames from virtual extinction through statutory licensing',* 35 Sw. U. L. Rev 401

Glasser, A.R. (1987) *'Video Voodoo: - Copyright in Video Game Computer Programs'*, 38 Fed. Comm. L.J. 103

Guttenbrunner, M., Becker, C., Rauber, A. & Kehrberg, C. (2008) *'Evaluating Strategies for the Preservation of Console Video Games'* Association for the Advancement of Artificial Intelligence, Vienna University of Technology

Mackenzie, S. (2010) *'Counterfeiting as corporate externality: intellectual property crime and global insecurity'* Crime Law and Social Change 54 21-38

McBride, S. & Smith, E. (19/12/2008) *'Music Industry to Abandon Mass Suits'*, Wall Street Journal. Retrieved 1st March 2012 from http://online.wsj.com/article/SB122966038836021137.html

McDonald, T.L. (September 1999) *'You Will Be Emulated: - Console Emulators are Not Piracy; They're Ingenuity at Work'*, Maximum PC September 1999

O'Brien, T. (09/04/2011) *'Switched's Comprehensive Guide to Videogame Emulators',* Switched. Retrieved on 25th February 2011 from http://www.switched.com/video-game-emulators/switched-ultimate-guide-retro-gaming/

Pollock, R. (August 2007) *'Forever minus a day? Some theory and empirics of optimal copyright'*, University of Cambridge. Retrieved 27th February 2012 from http://www.rufuspollock.org/economics/papers/optimal_copyright.pdf

PVC Museum (2005) *'Total Worldwide Console Hardware Sales'* retrieved on 25th February 2012 from http://www.pvcmuseum.com/games/charts/total-worldwide-console-hardware-sales.htm

LA «LEY SINDE»: UNA OPORTUNIDAD PERDIDA PARA LA REGULACIÓN DEL OCIO ONLINE EN ESPAÑA

Ercilia García Álvarez
Catedrática Facultad de Economía y Empresa Universidad Rovira i Virgili
Investigadora del Centro de Estudios y Recerca de Humanidades (CERHUM) - UAB

Jordi López Sintas
Profesor Titular de Universidad Facultad de Economía y Empresa Universidad Autónoma de Barcelona
Investigador del Centro de Estudios y Recerca de Humanidades (CERHUM) - UAB

Sheila Sánchez Bergara
Estudiante de Doctorado de la Universidad Rovira i Virgili

RESUMEN: Las nuevas tecnologías e Internet han transformado las experiencias de ocio y las formas de acceder y consumir bienes protegidos por la propiedad intelectual. Esta situación provoca tensiones entre los titulares de derechos de propiedad intelectual, los usuarios e intermediarios. Con el propósito de fortalecer la protección en el ciberespacio se aprueba la «Ley Sinde,» normativa aplaudida por unos y objetada por otros. En esta comunicación nuestro objetivo es cuestionar la eficacia de esta regulación como respuesta a la problemática del acceso y consumo de obras en Internet. Su contenido evidencia una desatención a las prácticas de ocio online a partir de las libertades de creación que la tecnología pone al alcance de los usuarios. Los derechos de las partes implicadas están en desequilibrio, no responde a la demanda de ocio online e impone cargas a los intermediarios. Es un remedio legal que obvia la eficacia de la arquitectura de la red como subterfugio para evadir las consecuencias jurídicas. Nuestra conclusión es que constituye una solución jurídico-formal que no responde a la complejidad del fenómeno porque se centra en la defensa a ultranza de una sola de las partes, además de ser insuficiente como mecanismo de regulación para las relaciones en el entorno digital.

PALABRAS CLAVE: ocio online, propiedad intelectual, Ley Sinde, regulación, nuevas tecnologías.

1. INTRODUCCIÓN

El ocio y las nuevas tecnologías siempre han estado relacionados, cada adelanto tecnológico ha repercutido en su concepto, formas de experimentación, acceso y organización (Bryce, 2001). A la relación ocio-nuevas tecnologías incorporamos el sistema de propiedad intelectual, en tanto regula las condiciones de acceso y transacción de bienes esenciales para las experiencias de ocio y cuya historia puede resumirse a partir de los principales adelantos tecnológicos. En el contexto actual la tensión entre intereses y derechos de las partes implicadas es creciente (de la Fuente & Ureña, 2006) y las soluciones jurídicas implementadas cuestionables.

La era digital ha transformado los espacios, actividades y organización de las experiencias de ocio, las personas interaccionan en nuevas comunidades de forma sincrónica o asincrónica al tiempo que permanecen en un espacio físico (Bryce, 2001). Las actividades de

ocio tradicional coexisten con las de ocio digital que en parte las incorporan al tiempo que existen otras propias del ciberespacio. Los tiempos también cambian, el ocio digital es más frecuente y se entremezcla con actividades laborales. En todo caso, cumple las mismas funciones que el tradicional, es decir, proporciona relajación, estimulación, escape, interacción social y desarrollo de la propia personalidad con repercusiones positivas para el bienestar (Bryce, 2001).

El incremento del ocio online también se evidencia en la importancia del acceso a Internet desde el hogar. Según los resultados del Eurobarómetro 362/2011 la media europea alcanza al 62% de los hogares con conexión y en España el acceso es de un 51%. Entre las actividades de ocio online más frecuentes según el Eurobarómetro 278/2007 destacan el intercambio de e-mails con 68%, la búsqueda de información sobre productos y eventos culturales y la preparación de las vacaciones ambas con 42% y la búsqueda de información sobre actividades deportivas y de ocio con 41%, la lectura del periódico con 39%, compra de productos culturales un 30%, escuchar la radio/música un 28%, descargar música gratis y compartir archivos con 27% y 26% respectivamente, los videojuegos ocupan el 25%, visitas a webs de museos y bibliotecas un 24 %, visitas a fórums y chats un 22%, consulta de blogs un 13% y un 9% destinado a la creación de webs y blogs propios. Estos datos, revelan el creciente interés y uso de las tecnologías e Internet para experiencias de ocio, en la mayoría de los casos relacionados con bienes de propiedad intelectual.

Al tiempo que transforma las experiencias de ocio, la era digital también permite manipular obras protegidas por la propiedad intelectual. Actividades antiguamente reservadas a profesionales y técnicos como: procesar, modificar, ampliar, reducir y copiar, están ahora al alcance de los usuarios. Por ello, se puede ser autor, editor, gestor e infractor al mismo tiempo o en diferentes momentos (Lipszyc, 2004). Estos hechos, se presentan como un desafío para la propiedad intelectual sustentada en el paradigma de la exclusividad. Una vez digitalizadas, las obras se convierten en bienes públicos desde una perspectiva económica y la escasez pierde toda importancia, de ahí que los fundamentos de la teoría de la propiedad tradicional no resuelvan con éxito las problemáticas del ciberespacio, puesto que la única limitación es la cantidad de bits que podemos almacenar (Murray, 2010).

Las oportunidades de las nuevas tecnologías para crear benefician a la cultura amateur que no es nueva ni originaria del ciberespacio, lo que sucede es que la red ha expandido su alcance a niveles extraordinarios que en el espacio real eran difíciles de obtener (Lessig, 2006). Según este autor, la remezcla ingeniosa de acontecimientos políticos o de canciones ha dejado de ser algo que solo podemos compartir con familiares y amigos. Así, Internet se presenta como un espacio con una asombrosa creatividad generada por los usuarios desde los blogs, las emisiones de podcast y videocast y las remezclas de contenidos –mashups– (Lessig, 2006).

Las respuestas a las nuevas vías de acceso y consumo de la propiedad intelectual han dado la espalda a la demanda, o si se prefiere, a los usuarios. A nivel internacional se ha promovido la implementación de una variedad de remedios procesales para la defensa de la propiedad intelectual en el ámbito online. Sin embargo según (Graber, 2011, p.22) existe una amplia brecha entre lo que la ley establece y lo tolerado por los intermediarios en el ciberespacio. En estas condiciones es necesario repensar los mecanismos que garanticen el

respeto de derechos constitucionales como la libertad de expresión y de recibir y comunicar información, teniendo en cuenta el poder de las estructuras tecnológicas como mecanismo de regulación (Graber, 2011).

En este contexto España ha reajustado el marco jurídico de la propiedad intelectual para responder a los compromisos internacionales y a las directivas europeas. Los titulares de derechos de propiedad intelectual cuentan con instrumentos de defensa en el ámbito civil, penal y administrativo (Padrós, 2011a) sin embargo, quedaban carencias por cubrir. Así, tras un arduo proceso de negociación parlamentaria se aprueba la Ley 2/2011 de 4 de marzo, de Economía Sostenible, cuya Disposición final cuadragésima tercera es la conocida como «Ley Sinde.» Con esta última denominación nos referiremos a la norma por economía y popularidad.

En esta comunicación nos proponemos analizar a partir del contenido de la «Ley Sinde» cómo se equilibran los derechos de las diferentes partes implicadas y las potenciales dificultades de su aplicación. Además incluimos las reacciones más representativas que a favor y en contra ha tenido. Nuestro propósito es demostrar que esta regulación es estrictamente una solución formal diseñada para salvaguardar monopolios en el mercado de bienes culturales siguiendo premisas jurídicas que desconocen las oportunidades tecnológicas.

2. DEBATE SOBRE LA REGULACIÓN DE LA PROPIEDAD INTELECTUAL ONLINE

En las relaciones por actividades de ocio online convergen distintos derechos que en ocasiones colisionan y en la actualidad son objeto de un intenso debate académico, legislativo, jurisprudencial y social. Las posturas adoptadas proponen un amplio espectro de posibles soluciones no siempre fundamentadas pero en todo caso reflejo de los intereses en juego. En el contexto internacional la tendencia ha sido reforzar la protección, imponiendo a los Estados obligaciones que en ocasiones sobrepasan sus condiciones para implementarlas (Ruse-Khan, 2009). A través del argumento de la innovación (Campbell & Picciotto, 2006) se ha justificado la propiedad intelectual como incentivo a la creación, salvaguarda de la cultura y promoción del desarrollo económico. En este sentido (Campbell & Picciotto, 2006) afirman que la propiedad intelectual se utiliza para reforzar el poder del mercado a través de la intervención del Estado. Y se justifica la configuración del sistema debido a que los beneficios exceden los costes que supone (Landes & Posner, 2006).

Frente a estas posturas se han desarrollado teorías alternativas para regular las relaciones en el ciberespacio. La escuela de los ciberlibertarios[1] sostenía que la naturaleza incorporal y descentralizada de la red solo podía ser regulada a través de su propio desarrollo orgánico con el consentimiento de la mayoría de los cibernautas (Murray, 2008). La escuela de los ciberpaternalistas[2] defiende la autorregulación a partir del código fuente como mecanismo de control sobre los individuos (Murray, 2008). En la propuesta de la Network Communi-

1 Más en: (Johnson & Post, 1996).

2 Más en: (Lessig, 1999).

tarian School se reconoce el poder de comunicación de la red y se incluyen otros mecanismos de regulación debido a su efectividad (Murray A., 2011). Por su parte, la regulación simbiótica (Murray, 2008) apuesta por un modelo que ofrezca a todos la oportunidad de intervenir, siendo clave la comunicación entre las partes.

Dentro de este debate a nivel europeo se ha optado por implementar soluciones legales del mundo físico al ciberespacio para la defensa de la propiedad intelectual online. En 2009, Francia con la Ley n°2009-669 de 12 de junio de 2009, conocida como Ley HADOPI instaura un mecanismo de protección que después de tres advertencias sanciona al usuario final por decisión jurisdiccional. España en 2011 aprueba la «Ley Sinde» centrada en los prestadores de servicios de la sociedad de la información como potenciales infractores. En ambos casos, se favorecen los intereses de las industrias de ocio y se implementan nuevas medidas contra el acceso y consumo de obras online.

La necesidad de regular el acceso y consumo de bienes protegidos por la propiedad intelectual en la red es evidente, el reto es obtener un resultado que responda a la complejidad del fenómeno, considere las transformaciones en los hábitos de ocio online y pondere adecuadamente los derechos en conflicto. La respuesta española es la conocida «Ley Sinde,» realmente la Disposición Final cuadragésima tercera de la Ley 2/2011. Su contenido modifica aspectos de tres normas jurídicas: la Ley 34/2002, la Ley 29/1998 y el Real Decreto Legislativo 1/1996. Con la entrada en vigor el pasado primero de marzo del Real Decreto 1889/2011 de 30 de diciembre por el que se regula el funcionamiento de la Comisión de Propiedad Intelectual comienza su aplicación.

Aunque de esta norma es posible realizar un análisis exhaustivo sobre las repercusiones de su contenido, a continuación nos centramos en los elementos de mayor relevancia para el ocio online. Primeramente, abordamos las partes implicadas, sus intereses y la ponderación de los derechos en conflicto. En segundo lugar, los problemas que previsiblemente tendrá su aplicación y por último, las posturas adoptadas respecto a la norma por las partes.

3. PARTES IMPLICADAS, INTERESES Y DERECHOS EN LA «LEY SINDE»

En este apartado ilustramos los principales sujetos implicados en conflictos relacionados con la propiedad intelectual en el ámbito online. Primeramente, los titulares de estos derechos por ser la parte que reclama una observancia estricta al tiempo que ejerce una importante presión a nivel internacional y nacional. Como contraparte más evidente incluimos a los usuarios, tanto personas naturales como jurídicas, para ambas la regulación de la propiedad intelectual supone costes y límites. Adicionalmente, incluimos a los prestadores de servicios de intermediación por el rol que desempeñarán en defensa de la propiedad intelectual. En ningún caso los grupos son homogéneos, por lo que nos limitamos a señalar las posturas más representativas.

Al autor como principal titular se le reconoce un derecho exclusivo que le faculta para explotar su creación por diversas vías y durante un extenso período de tiempo (art.20.1 b) CE.; art.2 y 26 TRLPI). Además del interés por el reconocimiento a la autoría y la integri-

dad de la obra, les preocupa contar con ingresos que recompensen el trabajo realizado y les permitan continuar creando. En igual situación se hallan los artistas intérpretes y ejecutantes, en su condición de titulares de derechos conexos (arts. 106-109 TRLPI). Sin embargo, en ambos casos, el denominador común suele ser la existencia de un vínculo contractual que repercutirá en el ejercicio de las facultades de explotación. Por regla general, el contenido económico de los derechos de autor y conexos se transfiere, de ahí que (Ruse-Khan, 2009) afirme que el principal interés de estos sujetos se dirige hacia las normas que garanticen la equidad en las condiciones de cesión, en el contenido de los contratos laborales y en los regímenes de regalías por licencias.

Incluimos a las sociedades de gestión colectiva en este apartado pues si bien no ostentan *per se* derechos de propiedad intelectual, en su condición de representantes de los titulares, desempeñan un rol muy activo en su defensa. En el contexto español se han convertido en monopolios de hecho (Padrós, 2011b) y a pesar de los beneficios reconocidos tradicionalmente a la gestión colectiva, también se han identificado problemas comunes a sus posiciones monopolísticas como limitaciones al desarrollo de mercados no tradicionales de explotación de obras, dificultades para que los usuarios gestionen eficientemente sus costes, alto nivel de litigio entre oferentes y demandantes y un incremento en los costes de transacción. Actualmente, las nuevas tecnologías e Internet ofrecen mecanismos alternativos a la gestión colectiva tradicional (Torres Padrosa & Delgado, 2011; Garcelon, 2009) que se han considerado amenzas en tanto proporcionan a los creadores nuevos mecanismos para ejercer y licenciar sus facultades patrimoniales (Navarro, 2011).

Las industrias de ocio son un grupo muy variado tanto por el tamaño de las empresas como por las actividades que realizan, sin embargo, como regla son titulares de derechos de propiedad intelectual (arts. 8; 97.1.2.4; 115-117; 121-123 y 126 TRLPI). Su principal interés consiste en recuperar sus inversiones y obtener un beneficio mediante la explotación de las obras y otras prestaciones. Por ello, defienden la observancia a ultranza de la propiedad intelectual a través del perfeccionamiento de los mecanismos de aplicación y sanción previstos en las normas jurídicas (Ruse-Khan, 2009). También han promovido la globalización de los estándares de protección en el marco de la OMC aunque los recursos para implementarlos y sus consecuencias difieren entre países (Drahos, 1997). En la agenda internacional, el debate sobre la protección y salvaguarda de la propiedad intelectual representa fundamentalmente los intereses de las multinacionales del ocio (Ruse-Khan, 2009).

Tanto Internet como las tecnologías digitales han repercutido en sus modelos de comercialización de obras basados en la realidad analógica. La sustitución del soporte físico por el digital implica transformaciones en la configuración de la cadena de valor, donde algunas estructuras empresariales dejarán de ser necesarias o sufrirán transformaciones muy profundas. El instinto de conservación se pone en evidencia a través de las posiciones más extendidas a nivel internacional, donde las grandes industrias persiguen mantener su *status quo* a toda costa (Ruse-Khan, 2009). No obstante, a pesar de las resistencias Dyson (1994) advertía a los creadores de contenidos que el principal reto sería decidir qué dar gratis y qué cobrar en la red, teniendo en cuenta lo que hacen los competidores y las expectativas de los clientes.

A pesar de los inconvenientes que supone el cambio de los modelos de negocio para el entorno digital, las industrias paulatinamente se verán forzadas a encontrar nuevos caminos porque lo que pueda ser digitalizado lo será y con ello las obras serán cada vez más fáciles de copiar y más difíciles de vender por más de su precio nominal (Krugman, 2008). Las industrias deberán adaptarse al entorno digital o de lo contrario perecerán (Bailey, 2006). Sin duda el actual sistema de propiedad intelectual expresa y protege la existencia de las industrias de ocio, no obstante, la oferta online no responde a la demanda cada vez más exigente.

Por otra parte y cada vez con mayor trascendencia en este tema se encuentran los proveedores de Internet, titulares del derecho de libertad de empresa (art. 38 CE.). En los últimos años algunos países han optado por incorporarlos a la salvaguarda de la propiedad intelectual y de este modo, eximirlos de responsabilidad subsidiaria o en segundo grado (Ruse-Khan, 2009). Ya sea para la identificación de supuestos infractores como para la suspensión del acceso, son los que cuentan con herramientas tecnológicas para ejecutar estas u otras medidas. Por regla general, se han opuesto a asumir este rol defendiendo la libertad de empresa, la neutralidad en la red, los derechos de los usuarios finales y resaltando los costes que les suponen estas actividades. No obstante, por mandato legal han asumido obligaciones de colaborar en la salvaguarda de la propiedad intelectual (Win & Jondet, 2009; Lucchi, 2011) en Francia, Reino Unido, Irlanda, Suecia y ahora España.

Los usuarios de bienes protegidos por la propiedad intelectual, cuando son personas naturales, suelen consumir estos bienes en actividades de ocio y son titulares de derechos como el de acceso a la cultura, la libertad de expresión y la libertad de recibir y comunicar información (art. 44.1; 20.1 a), d) CE.). Además, se benefician de las excepciones previstas para los derechos de propiedad intelectual (arts. 31-40 TRLPI). Dentro de este grupo, los intereses se centran en la ausencia de penalizaciones exorbitantes por prácticas de ocio cada vez más recuentes como la descarga de un archivo de música o la visualización online de una película sin autorización del titular de los derechos. Las posturas son tanto defensivas de sus derechos como de desarrollo de las excepciones previstas a través de mecanismos efectivos (Ruse-Khan, 2009).

Los casos de personas jurídicas como usuarios de propiedad intelectual en la red para el desarrollo de sus actividades profesionales o empresariales son cada vez más frecuentes. Por ejemplo, el uso de herramientas de comercialización y comunicación online es indispensable para mejorar la competitividad de las empresas. En el ejercicio de su derecho a la libertad de empresa (art. 38 CE.) incrementan su presencia en la red como canal de comunicación con sus actuales y potenciales clientes, co-creación de contenidos, cuidado de la reputación online, distribución y ventas. Estas actividades implican un incremento en el acceso a bienes protegidos por la propiedad intelectual, de los cuales no suelen ser titulares. El reforzamiento de los derechos de propiedad intelectual en la red les repercute en costes de transacción.

De lo expuesto hasta el momento, cabe resaltar que el acceso, consumo y creación de obras en la red son prácticas que generan colisiones entre los derechos de propiedad intelectual y los derechos de libertad de expresión, libertad de recibir y comunicar información, acceso a la cultura y libertad de empresa. La necesidad de regular estas relaciones es evidente, sin embargo, una solución conciliadora requiere analizar el fenómeno en su integridad. Para

ello se hace necesario conocer las relaciones que se entablan en la red, los cambios que han supuesto Internet y las nuevas tecnologías en las prácticas de ocio y en el consumo de obras. También sería recomendable anticiparse a las tensiones que entre estos actores se suscitan como resultado de derechos que se contraponen.

3.1. Cuestiones procesales con repercusiones para los derechos e intereses de las partes

En el contenido de la «Ley Sinde» existen varios aspectos relevantes que requieren de un estudio exhaustivo. En relación al tema abordaremos los que mayor cuestionamiento generan.

Creación de un órgano administrativo. La «Ley Sinde» apuesta por la existencia de un nuevo ente cuya única finalidad consiste en salvaguardar los derechos de propiedad intelectual en la red. Así, modifica el art. 158.4 del TRLPI establece la creación de la Sección Segunda de la Comisión de Propiedad Intelectual. Teniendo en consideración que ya existía tutela penal, civil y administrativa, esta última encomendada a la Comisión de la Propiedad Intelectual y el antiguo Ministerio de Cultura (Padrós, 2011a) a partir de una variedad de medidas preventivas, de sensibilización y normativas, la reestructuración la Comisión genera cuestionamientos sobre los costes y pertinencia de un nuevo órgano para su defensa.

Esta medida otorga ventajas a los titulares de propiedad intelectual en tanto les ofrece una vía alternativa a la jurisdiccional. En este contexto, supone perjuicios para los intermediarios y los usuarios. Respecto a los primeros tendrán que colaborar en el procedimiento asumiendo obligaciones. Los segundos, pueden ver limitado el acceso a obras para sus actividades de ocio online, sin que alternativamente cuenten con una oferta legal acorde a sus demandas y perfiles. Ambos grupos son titulares de derechos que sufren limitaciones y cuentan solamente con la tutela jurisdiccional con los costes en tiempo y dinero que le son inherentes. Lo cual refleja una preferencia por los derechos de propiedad intelectual respecto al resto de derechos involucrados.

Supuestos que generan responsabilidad. Ante la Sección Segunda podrá acudirse en caso de presunta vulneración de derechos de propiedad intelectual en el ciberespacio por parte de un prestador de servicios de la sociedad de la información siempre que éste actúe directa o indirectamente con ánimo de lucro o haya causado o sea susceptible de causar un daño patrimonial al titular (art. 158. 4 párrafo 2 TRLPI y art. 13.3 RD 1889/2011). En la delimitación de los supuestos de hecho que legitiman el uso de este mecanismo de defensa resalta el uso de la conjunción «o» para ampliar los casos, incluso algunos desestimados judicialmente.[3] Añadir el término «susceptible» permite incluir supuestos en los que el daño no se ha concretado pero existe riesgo de que suceda, lo cual supone la posibilidad de retirar contenidos o suspender el servicio *ex ante* del resultado dañoso.

Esta modificación faculta a los titulares de propiedad intelectual a iniciar el procedimiento siempre que acrediten por cualquier medio de prueba admisible en derecho la ex-

3 *Cfr.* Resoluciones judiciales: AC\2011\1630, JUR\2010\90760, JUR\2011\92416.

plotación lucrativa o no de la obra (art. 17.2 inc. c) RD 1889/2011). Esta previsión puede suponer limitaciones a los derechos de acceso y comunicación de información, acceso a la cultura y protección de datos, además de obviar que compartir obras es un hábito anterior a la era digital. Las nuevas tecnologías favorecen la masificación de estos comportamientos a los que la actual regulación pone barreras. Por una parte, impone obligaciones a los intermediarios en el procedimiento con los costes añadidos que supone para el desarrollo de sus actividades. Por otra parte, limita los recursos disponibles en la red para los usuarios, sin prever alternativas legales que los sustituyan. La regulación de la propiedad intelectual en el ciberespacio debe responder no solo a los intereses de los titulares de derechos de autor y conexos sino también a los nuevos hábitos de ocio online. Una vía podría ser repensar las excepciones a la propiedad intelectual desde la perspectiva del usuario que realiza actividades de ocio online.

Retirada de contenidos y suspensión del servicio. Contra los infractores se podrá ordenar la suspensión del servicio de la sociedad de la información o la retirada de contenidos (art. 8.1 e) Ley 34/2002). Junto a los supuestos ya previstos se adiciona «la salvaguarda de los derechos de propiedad intelectual.» Así se concede a un derecho de propiedad *sui generis* medidas previstas para la infracción de principios de naturaleza pública e interés general como la dignidad de la persona, la no discriminación, la protección a la infancia, la salud y la seguridad públicas, cuando son vulnerados en la red. Esta previsión refuerza la prevalencia de la propiedad intelectual frente a los derechos de usuarios e intermediarios cuyo ejercicio se limita cada vez que se refuerza la salvaguarda de aquélla.

Presunción de responsabilidad. También refuerza la posición de los titulares de propiedad intelectual la previsión del art. 20.1 RD 1889/2011. Iniciándose el procedimiento con un requerimiento al presunto infractor para que retire los contenidos, lo que supone una inversión de la carga de la prueba a costa de los prestadores de servicios de la sociedad de la información. Así, sobre quien todavía no ha sido declarado culpable pesa el deber de alegar y probar su inocencia. Cualquier otra acción u omisión supone un reconocimiento a la vulneración de derechos de propiedad intelectual.

Intervención de intermediarios. De modo coherente con la tendencia internacional (Graber, 2011) se incluye en el procedimiento a los prestadores de servicios de intermediación. En una primera fase, (art. 8.2 Ley 34/2002 y art. 18.1 RD 1889/2011) podrán ser requeridos para que identifiquen al prestador del servicio de la sociedad de la información[4] responsable de la supuesta infracción previa autorización judicial (art. 18.1 RD 1889/2011). Obtenida la cual, es obligación ineludible ceder a la Sección Segunda los datos que permitan su identificación inequívoca en el término de 48 horas desde la recepción del requerimiento. Tanto la ejecución de la solicitud como el tiempo concedido suponen cargas para estos sujetos, además de limitaciones al derecho de libertad de empresa para salvaguardar derechos de propiedad que prevalecen sobre el primero sin que consten razones que justifiquen esta elección. En una segunda fase, también podrán ser compelidos a intervenir en la ejecución

4 Contrario a lo establecido en la STJUE de 29 de enero de 2008, en el asunto C-275/06, respecto al suministro de datos personales.

de la sanción si el infractor no cumple voluntariamente. Según el art. 22.3 RD 1889/2011, cuentan con 72 horas para ejecutar la suspensión del servicio a partir de la notificación del auto judicial que autoriza la medida. Se impone así un rol activo a los intermediarios a través de obligaciones que suponen nuevas cargas técnicas y de recursos para responder a los requerimientos en términos breves sin que consten consideraciones sobre cómo aminorar las repercusiones para el libre desarrollo de sus empresas y los costes a asumir.

Como conclusión preliminar podemos afirmar que la «Ley Sinde» se diseñó para favorecer a los titulares de propiedad intelectual frente a usos no autorizados en Internet. Con este propósito, se crea un órgano específico para estos conflictos, un procedimiento exclusivo con plazos breves y nuevas obligaciones para los intermediarios. Esta regulación da a entender una preferencia por los derechos de propiedad intelectual respecto al resto de derechos implicados, cuyo resultado echa en falta un análisis sobre el proceso y los mecanismos de ponderación de derechos empleados. Tampoco resuelve las exigencias de los usuarios respecto al acceso de obras online para actividades de ocio, ni propicia cambios en los modelos de distribución y comercialización de la propiedad intelectual en el entorno digital a medio o largo plazo. Su contenido no ofrece soluciones a los reclamos propios de la indetenible incorporación de las nuevas tecnologías en la vida de las nuevas generaciones de personas y empresas.

4. APLICACIÓN DE LA «LEY SINDE»: POTENCIALES DIFICULTADES

La aplicación de la «Ley Sinde» exigía de desarrollo reglamentario, tanto para la creación del órgano como para la delimitación del procedimiento. En este sentido, el primero de marzo de 2012 entró en vigor el RD 1889/2011, por el que se regula el funcionamiento de la Comisión de la Propiedad Intelectual. A partir de esta fecha podrán presentarse solicitudes fundadas en la nueva regulación. Por la trascendencia del tema en el contexto nacional, en este apartado nos centramos en identificar los elementos que previsiblemente dificultarán su aplicación a partir del análisis de su contenido y de las alternativas tecnológicas que permiten infringirla.

Entre las diferentes fases del procedimiento, destacan plazos tan breves como 48 horas para la retirada voluntaria de contenidos (art. 20.1 RD 1889/2011), dos días para la práctica de pruebas, cinco días para conclusiones (art. 21 RD 1889/2011) y tres días para la resolución (art. 22.1 RD 1889/2011). De este diseño inquieta la falta de tiempo con que contará la Sección Segunda para conocer el caso y conformar un juicio objetivo e imparcial. Además de la inevitable interrogante de cómo podrán en la práctica cumplirlos de presentarse un elevado número de solicitudes simultáneamente.

También los plazos con que cuentan los intermediarios son breves, 48 horas para aportar la información que permita identificar a los supuestos infractores (art. 18.4 RD 1889/2011) y 72 horas para la suspensión del servicio (art. 22.3 RD 1889/2011). Tampoco quedan ajenos a los términos breves los Juzgados Centrales de lo Contencioso-Administrativo para autorizar la identificación del supuesto infractor cuentan con 24 horas,

dos días para convocar a audiencia a las partes y otros dos días para autorizar o denegar la ejecución de la medida (art. 122*bis* 1 Ley 29/1998). Resulta evidente que las exigencias de celeridad pueden de facto convertirse en un problema para el funcionamiento judicial. Además de imponer la prevalencia de estos asuntos respecto al resto de los sometidos a este órgano jurisdiccional[5].

No obstante, la previsible ineficacia de la «Ley Sinde» no está determinada en exclusiva por las dificultades de cumplir cabalmente todas sus fases, tampoco por los recursos legales que contra ella se han interpuesto como se verá más adelante. Su talón de Aquiles radica en obviar las posibilidades de sortear con tecnología sus consecuencias jurídicas. Es un hecho que los adelantos tecnológicos e Internet favorecen el consumo masivo de obras, la co-creación y nuevos espacios y experiencias de ocio online (Bryce, 2001) que una vez incorporados son difíciles de erradicar o modificar a través de prohibiciones legales. Con esta norma se obvian las salidas tecnológicas como mecanismo de regulación en la red (Graber, 2011) que permiten mantener los hábitos de ocio online incluso en supuestos de ilegalidad. La presunta ineficacia de la norma ante estos casos denota que el fenómeno se ha analizado parcialmente y sugiere su fracaso como solución ante infracciones a la propiedad intelectual en la red.

Una parte de los usuarios ha manifestado su oposición al contenido de la norma a través de herramientas tecnológicas. Transcurrido un mes de su aprobación estaba disponible en la red un recurso tecnológico para burlar su cumplimiento, el Manual de Desobediencia de la Ley Sinde (Hacktivistas, 2011). Con un lenguaje claro y explícito identifican cinco métodos con que cuenta el gobierno para cerrar una página web y las posibilidades de sortear la clausura según se trate de un usuario o un *webmaster*. Como ejemplo de oposición desde la sociedad civil se propone demostrar a partir de herramientas tecnológicas la ineficacia de esta regulación, ofreciendo nuevos caminos para continuar creando y compartiendo en la red.

Las dificultades de aplicar normas jurídicas sin tener en cuenta las peculiaridades del ciberespacio pudieron constatarse en el experimento realizado por los abogados David Bravo y Javier de la Cueva. El pasado septiembre en el marco del festival de cine de San Sebastián, mientras Bravo ofrecía una charla, solicitaron a través de Twitter la colaboración de los cibernautas para crear una página web de enlaces. El propósito era demostrar la ineficacia de la «Ley Sinde» (Otto, 2011) antes de su entrada en vigor. El resultado superó las expectativas, en apenas una hora se crearon 20 páginas de descargas con cientos de enlaces cada una.

Por parte de los intermediarios también ha habido oposición a través de las herramientas tecnológicas, en tanto los cambios normativos les exigen reajustes en el desarrollo de sus empresas. Por ejemplo, Google para poder dar respuesta a los requerimientos judiciales, en especial en relación a la retirada de contenidos, ha cambiado los dominios de los blogs creados en Blogger de «.com» a «.es, .fr, .it» según el país que corresponda. Sin embargo, al

5 Más si se tiene en cuenta que la Ley 29/1998 ya contiene un procedimiento sumario especial para la protección de derechos fundamentales.

propio tiempo que explica los motivos del cambio, ofrece a los usuarios un recurso para saltarse esta restricción colocando al final de la url «/npr.» En este caso, nuevamente las herramientas tecnológicas se convierten en un subterfugio a las restricciones legales. Así, de ahora en adelante podremos encontrar blogs en doble versión (Cano, 2012).

Por último y sin que pretendamos exhaustividad de ejemplos, destacar que a nivel empresarial desde el sector tecnológico es posible ampliar los usos de dispositivos ya existentes para continuar en tiempos de ocio creando y compartiendo aunque esté prohibido. Por ejemplo, una herramienta que puede ser utilizada para burlar el cierre de páginas web es el disco duro en red (NAS). Constituye un sistema que permite almacenar información en una nube privada a través de una unidad de disco propia que se ha comprado y se tiene físicamente. Permite adjuntar y borrar información, tienen una amplia capacidad de almacenamiento y podría convertirse en una alternativa para el acceso a obras a prueba de intrusos (Alonso, 2012). Si se optara por ellos, la demanda se incrementaría con repercusiones positivas para este sector.

5. LA «LEY SINDE»: ENTRE VÍTORES Y ABUCHEOS

Durante todo el proceso de tramitación parlamentaria y elaboración de la norma las partes han mantenido sus posturas y argumentos. Resulta evidente a quiénes beneficia y a quiénes perjudica esta regulación. Entre los vítores más significativos está el emitido por la United States Trade Representative (USTR) en la publicación anual del Special 301 Report. Este informe recoge el estado de la protección de la propiedad intelectual en los diferentes socios comerciales de Estados Unidos y España desde 2008 forma parte de la Watch List. Sin embargo, las acciones realizadas a inicios de 2011 han sido reconocidas (USTR, 2011, pp. 39-40):

> «Spain remains on the Watch List. The United States welcomes the recent passage of legislation that will provide a mechanism for rights holders to remove or block access to infringing content online. Spain has demonstrated a serious commitment to addressing piracy over the Internet with this initiative. The United States will monitor implementation of the legislation and urges Spain to ensure that it addresses all forms of piracy over the Internet and that it provides for the swift removal of infringing content. The United States also urges Spain to continue to work to address additional concerns about piracy over the Internet, including the inability of rights holders to obtain identifying information necessary to prosecute online IPR infringers. Additionally, a 2006 Prosecutor General Circular that appears to decriminalize illegal peer-to-peer file sharing of infringing materials remains of concern. Delays in the adjudication of cases are common within Spain's judicial system, and judges do not appear to impose criminal penalties for IPR infringement crimes. The United States looks forward to continuing to work with Spain to address these and other concerns.»

El texto es claro, tanto por lo que se espera de España como por las carencias que debía suplir en la protección a la propiedad intelectual en Internet. Y después de cuatro años seguidos entre los países de la Watch List, en el Special 301 Report de 2012 España no ha sido incluida. Desde esta perspectiva, la Ley Sinde ha sido todo un éxito. En el ámbito nacional, las sociedades de gestión colectiva también han apoyado la normativa e incluso en ocasiones

la han considerado «light»,[6] han creado coaliciones[7] para incrementar la presión y encargan estudios[8] periódicos sobre el consumo de propiedad intelectual online para justificar sus exigencias. Consecuentemente, son pioneras en la presentación de denuncias con la entrada en vigor de la norma (Romero, 2012).

Entre los detractores más fervientes se hallan los usuarios, el desacuerdo con el contenido de la norma no se ha hecho esperar. Así, mediante soluciones tecnológicas como el Manual de Desobediencia a la «Ley Sinde» o a través de iniciativas previas a la «Ley Sinde» pretenden mantener las prácticas de acceso y uso de contenidos en el ciberespacio (Hacktivistas, 2011, p. 55), las más significativas:[9]

- Tools: Manual en construcción de herramientas de hacktivismo.
- Telecomix Crypto Munition Bureau: Wiki con extensa documentación sobre anonimato en Internet, tanto para usuarios como para proveedores de servicios.
- HerdictWeb: Proyecto colaborativo que registra las webs que están bloqueadas en todo el mundo.
- Streisand.me: Proyecto para la creación de servidores espejo (*mirrors*) de contenidos censurados en Internet.

Estas salidas tecnológicas para evadir normas jurídicas implican el uso de aplicaciones diferentes e incluso la elección de proveedores de servicios fuera del territorio español. Con ellas, hay ventajas para nuevos sujetos y potenciales amenazas para los intermediarios que pueden ser sustituidos por otros que estén en condiciones de prestar los servicios demandados. De ser el caso, nuevas tensiones pueden surgir en el futuro. Las polémicas que suscita este tema continúan creciendo, indubitadamente las soluciones adoptadas no han sido satisfactorias para todas las partes. No obstante, también han empleado instrumentos legales para oponerse a la norma, así la Asociación de Internautas ha impugnado el RD 1889/2011 ante el Tribunal Supremo (Internautas, 2012) junto a su suspensión cautelar. Entre los argumentos para sustentar el recurso esgrimen las limitaciones que puede significar esta norma para el correcto ejercicio de la libertad de información y expresión. Lo cual evidencia que los usuarios están empleando todos los mecanismos a su alcance para obtener el reconocimiento a sus demandas. Sin embargo, el pasado mes de mayo el alto Tribunal ha declarado improcedente el recurso interpuesto.

Por otra parte, también se oponen a la actual regulación los intermediarios, las compañías de acceso a Internet a través de Redtel, asociación que agrupa a principales operadores

---

6 *Vid.* Declaraciones del ex Presidente de la SGAE. Disponible en: http://www.rtve.es/noticias/20110112/sgae-confia-que-ley-sinde-salga-adelante-porque-light/394503.shtml. Consultado el 15/03/2012.

7 Coalición de Creadores e Industrias de Contenidos, grupo de presión formado por: EGEDA, Promusicae, SGAE, FAP, ADIVAN y ADICAN.

8 Informe sobre piratería y hábitos de consumo de contenidos digitales en España (1er y 2do semestre 2010), realizado por la Consultora IDC.

9 Más en: Manual de Desobediencia a la Ley Sinde (p.55) que proporciona los enlaces a cada uno de estos proyectos.

de telecomunicaciones con red propia como ONO, Orange, Telefónica y Vodafone, que han ejercido presión durante todo el proceso de negociación del contenido de la «Ley Sinde» y con posterioridad a su aprobación (Muñoz, 2010). Como principales argumentos sostienen su preferencia por órganos jurisdiccionales, la complejidad e ineficacia del procedimiento, el incremento de los litigios y el riesgo de pronunciamientos contradictorios (Muñoz, 2010).

También han expresado su oposición a la norma, la Red de Empresas de Internet (REI)[10] y la Asociación Española de la Economía Digital (Adigital)[11]. A pocos días de la entrada en vigor del reglamento han interpuesto un recurso ante el Tribunal Supremo (REI, 2012) y solicitaron como medida cautelar la suspensión del procedimiento de salvaguarda de los derechos de propiedad intelectual. Sus posturas las fundamentan en las limitaciones que supondría para el desarrollo de empresas e iniciativas con base digital o tecnológica en el contexto español. Este hecho evidencia que existen nuevos sectores empresariales que se oponen a la actual regulación de la propiedad intelectual por las repercusiones que supone para su desarrollo en Internet. Así, aunque el discurso oficial se centra en enfrentar a internautas e industrias de ocio, las normas de propiedad intelectual estrictamente concebidas para salvaguardar los intereses de estas últimas repercuten negativamente en otros sectores empresariales.

6. CONCLUSIONES

El ocio online y la utilización de Internet como canal de comunicación, distribución y venta son fenómenos en crecimiento e indetenibles. Ante el incremento de vulneraciones a la propiedad intelectual en la red, España ha optado por diseñar una herramienta legal con privilegios para una sola de las partes. La «Ley Sinde» sigue las exigencias internacionales en pos de reforzar la protección a los titulares de propiedad intelectual. Sin embargo, queda pendiente una salida satisfactoria para la demanda de ocio online que considere los nuevos roles de los usuarios en el ciberespacio. Por ejemplo, motivar y/o compeler a las industrias de ocio a reajustar sus modelos de negocio al ciberespacio o repensar el contenido de las excepciones a la propiedad intelectual en actividades de ocio online son tareas pendientes.

Esta regulación pretende erradicar los usos no autorizados de propiedad intelectual en Internet a través de la retirada de contenidos o la suspensión del servicio. Pero a pesar de reforzar la protección de la propiedad intelectual en la red, sus consecuencias pueden ser evadidas con subterfugios tecnológicos. La respuesta jurídica se erige como instrumento estrictamente formal que no consigue equilibrar los derechos de todas las partes implicadas al inclinar la balanza desmedidamente a favor de los titulares. Así, los derechos de consumi-

10 Su núcleo fundador está formado por 14 compañías cuyo objetivo es impulsar el desarrollo de Internet en España y defender los intereses de las empresas que desarrollan contenidos en su más amplio sentido. Véase: http://redempresasinternet.es/que-es-rei. Consultado el 15/marzo/2012.

11 Asociación que integra a una extensa variedad de empresas e instituciones cuyo objetivo en común es el interés en el desarrollo de la economía digital. Véase: http://www.adigital.org/quienes-somos/quienes-somos. Consultado el 15/marzo/2012.

dores e intermediarios han sido preteridos y a falta de una regulación satisfactoria para todas las partes, el ocio online se mantendrá en terrenos de ilegalidad.

7. BIBLIOGRAFÍA BÁSICA

Alonso, L. (2012). *Los archivos de discos duros en red, ahora accesibles desde Internet.* Consultado el 9/marzo/2012, en El País.com: http://tecnologia.elpais.com/tecnologia/2012/02/24/actualidad/1330069796_430231.html.

Bailey, C. W. (2006). Strong Copyright + DRM + Weak Net Neutrality = Digital Dystopia? *Information Technology and Libraries*, 116-139.

Bryce, J. (2001). The technological transformation of leisure. *Social Science Computer Review, 19*(1), pp. 7-16.

Campbell, D., & Picciotto, S. (2006). The acceptable face of intervention: intellectual property in posnerian law and economics. *Social and Legal Studies*, 435-452.

Cano, R. J. (2012). *Blogger, en doble versión para evitar la censura.* Consultado el 9/marzo/2012, en El País.com: http://tecnologia.elpais.com/tecnologia/2012/02/02/actualidad/1328204537_633652.html.

De la Fuente Soler, M., & Ureña Salcedo, J. A. (2006). Las entidades de gestión de los derechos de propiedad intelectual: la necesidad de una revisión general del sistema. A A. Boix Palop, & G. López García, *La autoría en la era digital: industria cultural y medios de comunicación* (p. 131-166). Valencia: Tirant lo Blanch.

Drahos, Peter. (1997). Thinking strategically about intellectual property right. Telecomunications Policy, 21(3), pp. 201-211.

Dyson, Esther. Intellectual Property on the net. Consultado el 22/junio/2011 en Release 1.0 Monthly Report: http://cdn.oreilly.com/radar/r1/12-94.pdf.

Garcelon, M. (2009). An information commons? Creative Commons and public access to cultural creations. *New Media and Society*, 11(8), pp. 1307-1326.

Graber, C. B. (2011). *Internet Creativity, Communicative Freedom and Constitutional Rights Theory Response to «Code is law».* Consultado el 15/febrero/2011, en Selected Works: http://works.bepress.com/christoph_graber/1/.

Hacktivistas. (2011). *Manual de Desobediencia de la Ley Sinde.* Consultado el 30/mayo/2011, en Traficantes de sueños: http://www.traficantes.net/index.php/libreria/catalogo/libros/Manual-de-desobediencia-a-la-Ley-Sinde.

Internautas, A. d. (2012). *La Asociación de Internautas impugna la Ley Sinde Wert y pide su suspensión cautelar.* Consultado el 9/marzo/2012, en Asociación de Internautas: http://www.internautas.org/html/6962.html.

Krugman, P. (2008). *Bits, Bands and Books.* Consultado el 25/mayo/2011, en The New York Times: http://www.nytimes.com/2008/06/06/opinion/06krugman.html?_r=1&oref=slogin.

Landes, W., & Posner, R. (2006). La estructura económica de la propiedad intelectual e industrial. Madrid: Fundación Cultural del Notariado.

Lessig, Lawrence. (2006). Code: version 2.0. New York: Basic Books.

Lipszyc, Delia. (2004). Nuevos temas de derecho de autor y derechos conexos. Argentina: UNESCO-CERLALC-ZAVALÍA.

Lucchi, N. (2011). *Regulation and Control of Communication: The French Online Copyright Infringement Law (HADOPI).* Consultado el 6/junio/2011, en Social Science Research Network: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1816287.

Muñoz, R. (2010). *Los operadores advierten de que el cierre de webs atascará los juzgados.* Consultado el 1/junio/2011, en El País.com: http://www.elpais.com/articulo/cultura/operadores/advierten/cierre/webs/atascara/juzgados/elpepicul/20101015elpepicul_3/Tes.

Murray, A. (2011). *«Internet Regulation» Handbook on Regulation.* Edward Elgar.

Murray, A. (2010). *«The World of Bits» Information Technology Law: The Law and Society.* Ed. Andrew Murray. Oxford: Oxford University Press.

Murray, A. (2008). Symbiotic Regulation. *John Marshall Journal of Computer and Information Law* , 207-229.

Murray, A. D. (2003). Regulation and Rights in Networked Space. *Journal of Law and Society*, 187-216.

Navarro, Fernando. (2011). Reportaje: vida & artes. Compartir la música para defenderla. Consultado el 18/mayo/2011, en El País.com: http://www.elpais.com/articulo/sociedad/Compartir/musica/defenderla/elpepisoc/20110518elpepisoc_1/Tes.

Otto, C. (2011). *Cómo demostrar en una hora la ineficacia de la ley Sinde.* Consultado el 17/septiembre/2011, en ElConfidencial.com: http://www.elconfidencial.com/tecnologia/2011/09/16/como-demostrar-en-una-hora-la-ineficacia-de-la-ley-sinde-1064/.

Padrós Reig, C. (2011a). Debilidades y retos del régimen jurídico vigente de protección de la copia privada. A C. Padrós Reig, & J. López Sintas, *El canon digital a debate. Revolución tecnológica y consumo cultural en un nuevo marco jurídico-económico* (p. 169-246). Barcelona: Atelier.

Padrós Reig, C. (2011b). Los monopolios de gestión de derechos colectivos de propiedad intelectual ante las autoridades españolas de defensa de la competencia. A C. Padrós Reig, & J. López Sintas, *El canon digital a debate. Revolución tecnológica y consumo cultural en un nuevo marco jurídico-económico* (p. 247-280). Barcelona: Atelier.

REI. (2012). *REI y Adigital interponen un recurso contra la ley Sinde-Wert ante el Tribunal Supremo.* Consultado el 9/marzo/2012, en # Rei: http://redempresasinternet.es/categoria/noticias-rei.

Romero, P. (2012). *Cultura confirma las primeras 'denuncias' por la Ley Sinde.* Consultado el 15/marzo/2012, en ELMUNDO.es: http://www.elmundo.es/elmundo/2012/03/07/navegante/1331117567.html.

Ruse-Khan, H. G. (2009). *IP Enforcement Beyond Exclusive Rights.* Consultado el 6/junio/2011, en Social Science Research Network: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1445292.

Special Eurobarometer 278. European Cultural Values. (September/2007). Consultado el 29/junio/2011, en http://ec.europa.eu/public_opinion/archives/ebs/ebs_278_en.pdf.

Special Eurobarometer 362. E-Communications Household Survey (July/2011). Consultado el 26/abril/2012, en http://ec.europa.eu/public_opinion/archives/ebs/ebs_362_en.pdf.

Torres-Padrosa, V.; Delgado-Mercé J. (2011). Alternativas para la autogestión de los derechos de autor en el mundo digital. *Profesional De La Información*, 20(1), pp. 61-70.

USTR. (2011). *2011 Special 301 Report.* Consultado el 1/junio/2011, en Office of the Unite State Trade Representative: http://www.ustr.gov/about-us/press-office/reports-and-publications/2011/2011-special-301-report.

Win, J., & Jondet, N. (2009). A «New Deal» for End Users? Lessons from a French Innovation in the Regulation of Interoperability. *William and Marie Law Review* , 547-576.

6

THE DIGITAL CLOUD RECORDER: MODERN VCR OR NEW INTERMEDIARY?

Robin Kerremans
Legal Researcher
Interdisciplinary Centre for Law and ICT (ICRI),
Catholic University of Leuven (KULeuven), Belgium

ABSTRACT: Digital technologies, especially broadband technology, create opportunities for new services to emerge. A good example of such a new service in the market of audiovisual content is the so-called «Digital Cloud Recorder» (DCR). How should such a new «device» or service be perceived from a –Belgian– copyright point-of-view? Does the actual legal framework offer the right level of clarity to answer business-relevant questions? In this paper I will discuss the difficult relation of the DCR with traditional copyright concepts: the exceptions for private copying and temporary technical copies, cable retransmission and communication to the public and conclude that not all questions asked can be resolved with a simple yes or no answer. As with many copyright-related issues, the DCR and the entrepreneur wishing to bring it to the market will have to face the considerable risk of legal uncertainty.

KEYWORDS: digital cloud recorder, copyright, private copy, temporary technical copy, public communication, belgium.

1. INTRODUCTION

Digital technologies, especially broadband technology, create opportunities for new services to emerge. These new services, and the service providers who come with them, often have to secure their place in a given market, not only in the sense that they have to gain market share like any viable market player, but also, and perhaps more importantly, in the sense that they have to become accepted as a legitimate business. While this first fight will be fought against competitors, the latter will often be fought against parties who could be partners: other market players in a vertical relation to the new service provider, legislators and consumers. In converging markets, such as the market for audiovisual content delivery, it is however, difficult to determine positions: a partner today could become a competitor tomorrow and vice-versa.

A good example of a new such service in the market of audiovisual content is the so-called «Digital Cloud Recorder» (DCR). As an alternative to the decoding, the recording and the storage of audiovisual content through a set-top-box provided by a telecom provider, new service providers are offering similar, but often extended services via «the cloud».

In my paper I will discuss the difficult relation of the DCR with traditional copyright concepts: the exceptions for private copying and temporary technical copies, cable retransmission and communication to the public. Since the introduction of the European Co-

pyright Directive[1] (hereinafter referred to as the Copyright Directive), Belgium brought its national copyright legislation in line with the European standards. The question at hand is if the wording of this legal framework (both in the Directive and the national law) allows for DCR providers to roll out their business in Belgium (part 3). Before, I will provide a brief overview of the existing cloud technologies around the world, designed for the consumption of audiovisual content (part 2).

2. TECHNOLOGIES, SERVICES AND JURISDICTIONS – A BRIEF OVERVIEW OF CASES AROUND THE WORLD

In today's world, cloud services related to audiovisual content exist in many forms throughout many countries. Although they are all using the internet as a tool to view, record, store and even select content, important differences can be noticed with regard to the functionalities they offer.

2.1. TVCatchup (UK)

TVCatchup Limited is an internet-based service, that streams UK broadcast television programs in real time («live») to computers and smartphones («screen shifting»). However, the name TVCatchup («catch-up») is contradictory, since the service does not allow users to view programs at another time other than the original live broadcast. Therefore, there is no elaborated copy and permanent storage system in place. However, during the process of streaming live content to the user, a small amount of data from the video stream is held in the memory of the TVCatchup servers (the cloud). Users of the TVCatchup service must create an account with login details. Viewers can only receive access to content which they are already legally entitled to watch by means of their television license. The use is restricted to the country of residence (the service can locate the user's geographic location and refuse access if necessary). The input signals of TVCatchup are the normal terrestrial and satellite broadcast signals transmitted by the different television broadcasters. The signals are captured via an aerial and a satellite dish and then processed through a set of servers with software to change the format to digital («format-shifting») and encrypt the stream. TVCatchup is financed via advertisements before the live stream begins and via so-called «In-skin advertising», which are advertisements surrounding the live stream. The advertisements incorporated in the live stream (as part of the original broadcast) remain untouched.

2.2. Wizzgo (FR)

Wizzgo is also an internet-based service offering free copies of French free-to-air digital television channels. By installing a software package (iWizz) on one's computer a registered

1 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *Official Journal* L 167 , 22/06/2001 P. 0010 - 0019

user can select a program from the digital program guide on the Wizzgo website. Wizzgo then creates an encrypted copy, which only the individual user can decrypt via the iWizz software. The key difference between TVCatchup and Wizzgo is the fact that the latter offers the possibility to watch programs at a later time than the original broadcast («time-shifting»). Wizzgo is also funded by advertisement revenues.

2.3. Cablevision (USA)

A similar copy and cloud storage provider is the US-based company Cablevision. Like Wizzgo, they allow users access to content previously aired by cable broadcasters, which they have recorded and stored on their own servers. Cablevision users can access the content through their cable subscription with Cablevision, via their home television set, using only a remote control and a standard cable box (or «set-top-box») equipped with the special DCR software. The main differences with the two previous services is the fact that Cablevision operates via the traditional television screen and that Cablevision is both television operator and DCR-service provider.

2.4. TV Now (Australia)

TV Now is one of the most recent players to join the DCR market. The Australian-based company began offering the service in July 2011 to private and corporate customers. The service provides the user the ability to record free-to-air television programs and watch them on any of four compatible devices, namely: pc's, Apple, Android, and 3G devices. TV Now requires the user to click a virtual «record» button for a program in the service's electronic program guide. The TV Now service then creates an individual copy of that program in the four different formats. These copies are stored in the cloud for 30 days following the airing of the original broadcast. By clicking a virtual «play» button, the TV Now software starts streaming the program in the appropriate format to the user's device. The program cannot be downloaded and cannot be viewed in a live stream (only Apple device users can watch in a «near-live» stream, meaning that they can view the recording before the original broadcast is finished).

2.5. Relevant characteristics of DCR-services – Copyright question…

On the basis of the audiovisual cloud services described above it is possible to deduct three operational criteria in order to categorize the different services on the market: format-shifting, screen-shifting and time-shifting.

First of all there is the rather technical criterion of «format-shifting». Format-shifting refers to the technical procedure to change the video stream to a technical standard which can be received by the equipment of the user. Historically, format-shifting simply indicated the switch from analog to digital. Nowadays, most original video streams sent out by broadcasters are already digital, destined to be captured by specific set-top-boxes and television sets. In order to be viewed by other devices some format-shifting between digital formats is necessary to deliver an even digital stream to other devices, for example MP3, MP4, and 3G. Therefore, the term format-shifting now refers to all kinds of format-shifts, from analog

to digital, from one digital format to another, from free-to-air to encrypted. All of the previously described services use, to a certain extent, methods of format-shifting.

Secondly, we noticed that some DCR services provide what we could call a «screen-shifting» option, while others do not. Television broadcasts are traditionally viewed through television sets. However, technological convergence enables cloud service providers to deliver content broadcasted for television to other «screens», such as PC-screens, Apple-screens, mobile screens, etc. Although screen-shifting also often requires a format-shift, these two criteria are not completely identical. Also between identical screens format-shifting might be necessary. For that reason, we must identify it as separate criteria.

Thirdly and most importantly, there is the time-shifting criterion. Some services allow the user to watch the original broadcast in real-time, at the same time as the original live broadcast, while others allow the user to record the program in order to watch it at a more convenient time in the future (time shift or near-live). In the case of time-shifting, limitations with regard to the time a record can be stored or the times a broadcast can be watched are often brought into the forefront. Nonetheless, it is this third criterion which poses many copyright questions.

The combination of differentiators results in the following table, categorizing the previously described services.

	Time-shifting	**Live streaming**
Screen shifting	Wizzgo / TVNow	TVCatchup
Original screen	Cablevision	/

Note: Since all of these services require format shifting to a certain extent, this differentiator is irrelevant in the light of categorization. Therefore, it is not referenced in the table.

For now, there is no DCR service provider in the Belgian market. Therefore, our legal analysis is simply hypothetical. For the purpose of this paper we decided to conduct this hypothetical analysis using a «full option» service, such as Wizzgo and TVNow, combining format-shifting, screen-shifting and time-shifting functionalities.

3. FITTING DCR INTO BELGIAN COPYRIGHT LAW: VCR-WISE OR CABLE-WISE?

In this section we assess how a DCR-service with the relevant characteristics as described in the previous section could be perceived from a Belgian copyright point of view.

3.1. What is the legal status of the recording made by a DCR?

The recording made by a DCR qualifies without a doubt as a reproduction in the sense of the Belgian Copyright Act (hereinafter referred to as BCA)[2], harmonized by the Copyright Directive. The crucial question here is: who makes the copy?

2 Wet 30 juni 1994 betreffende het auteursrecht en de naburige rechten, *B.S.* 27 juli 1994 (BCA)

The DCR could, in essence, be compared with a system in which multiple VCR-recorders are recording every television channel to which an individual viewer has legal access, 24 hours a day (via free-to-air channels, cable subscription or otherwise). The BCA includes a specific copyright exception for private copying[3], enabling the making of such copies without prior consent of the right holders. We assess if a DCR would meet all the legal conditions of this exception.

Firstly, in most cases only the content a customer legally receives on the basis of a subscription with a digital television provider or on another TV license is recordable by the DCR. If we assume this would also be the case in our Belgian hypothesis, such a precondition would make the DCR compliant with the condition that the source of the private copy must be «*legally disclosed*»[4]. The scope of this provision (legal disclosure) refers to the author's moral right of disclosure and thus most certainly also implies legal disclosure in a stricter sense, notably non-copyright infringing disclosures.

Secondly, with regard to the nature of the content, the private copy exception covers audiovisual content, which is in most cases the predominant type of content a DCR is focusing on. Under the terms of the Copyright Directive all types of works should fall within the scope of the exception anyway. In Belgium, such a broader private copy exception has been implemented, but still waiting for the relevant Royal Decrees to make it applicable[5]. Audiovisual works (together with phonograms) have been implied in the Belgian exception since before the implementation of the Copyright Directive.

Thirdly and most importantly, the copy should be «*made within the family circle and used therein*» (Belgium). A traditional, narrow interpretation of this phrase would exclude a DCR from this exception. After all, a recording by a DCR is technically created by the cloud service provider. The customer has no physical recording device, like a digibox or a DVR at home when he uses a DCR. However, the cloud service provider in most cases only starts recording if the individual customer instructs it to do so. This instruction could be given in different ways, such as the push on a record button on a remote control or through a virtual interface. Another way in which instructions could be given could be in the form of a unique power of attorney, mandating the service provider to record all the programs that a user is entitled to watch on the basis of their TV license. The Belgian Supreme Court[6] confirmed,

3 Art. 22, §1, 5° BCA

4 Art. 22, §1 BCA. This is a general condition for all copyright exceptions in Belgium.

5 This new Royal Decree should contain a formula for a fair distribution of this remuneration between the right holders of different types of works. Previously, only right holders of audiovisual works and phonograms were included in the compensation regime. A distribution system between these two types of right holders has been in place for years. Under the new regulation authors of all types of works (written works, photographs, graphic works, etc.) are entitled to receive payment. How the division of the remuneration between all these types of right holders should be organised is the subject of continuing discussions between the collective rights management organisations of these right holders, delaying the enactment of the Royal Decree.

6 Cass., 27 May 2005, A&M, 2005, p.414, confirming Ghent, 16 June 2003, R.A.B.G., 2004, p.225, note Brison, F.

in a case of physical copy shops, that a third party providing the technical means to make the copy is not the actual «copier» in the sense of the private copy exception. In this case the copy shop did not make a copy at all; it just assisted an individual in making a private copy, allowed by the private copy exception. More importantly, an advice of the European Commission accompanying the final version of the Copyright Directive[7] clearly states that the formulation of the private copy exception in the Directive («*by a natural person for private use*», our highlight) includes the possibility that the copy is made «*for and on behalf of a natural person for private use.*» The Commission clarifies that this refers to third parties «*providing the means, technical or otherwise for the making of such copies*», if this copying has been done for «*ends that are neither directly or indirectly commercial.*»

Regarding the previously described TVNow service, the Federal Court of Australia[8] confirmed that it is the customer who «makes» the copy, not the DCR-service provider. Of course, in order to make a recording with TVNow, the Australian customers still need to select the programs they want to record and click on the virtual «record» button on a digital user interface. Therefore, a single general mandate given to a DCR-service provider by his customers to record everything might not be the safest path from a legal perspective. Although the instruction to «continuously press the «rec»-button» could perfectly qualify as a mandate, and has indeed been accepted by the European Commission as a valid way to exercise the private copy exception, a judge might still conclude that a more «active» intervention of the customer (such as selecting and pressing the «record» button) is required in order to fulfill the conditions of the exception. In our opinion however, such a rather conservative interpretation would hamper new technological evolutions and the creation of new business opportunities and create redundant inconvenience for consumers.

General terms and conditions of digital television contracts in Belgium often limit the right of the customer to make private copies of the broadcasts transmitted to them. A common clause which can be found in almost all these standard contracts, states that such a copy should be made by the customer himself *and not by a third-party*. Does this clause overwrite the legal exception? In Belgium, copyright exceptions are mandatory[9]. This means that they cannot be altered by contract. Contractual clauses changing the scope of an exception are null and void, unless they are situated in an on-demand context. Since a DCR

7 Commission Opinion pursuant to Article 251(2)(c) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a Directive of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society, Amending the proposal of the Commission pursuant to Article 250(2) of the EC Treaty, COM(2001) 170 final, Brussels, 29 March 2001. Retrieved March, 16th, 2012 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52001PC0170:EN:PDF

8 *Singtel Optus Pty Ltd v. National Rugby League Investments Pty Ltd (No 2)* [2012] Federal court of Australia, 34, 1 February 2012, similar interpretations can be found in *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d121 (Court of Appeal, 2d Cir.), 4 August 2008 and *RecordTV Pte Ltd v MediaCorp TV Singapore Pte Ltd* [2010]SGCA 43

9 Art. 23bis BCA

is only recording linear broadcasts and does not touch upon the on-demand boutique of any television provider, we believe that the exception for private copying cannot be limited in this respect. Assuming that the right to mandate the technical creation of a private copy to a third party service provider is an integrated element of the right to private copy, the general conditions limiting this option to mandate will be null and void. According to the advice of the European Commission this option to «outsource» the creation of the private copy stems from the *wording* of the Copyright Directive itself, and could thus be seen as an integrated element thereof. If the option to mandate is comprised in the exception itself - and the Belgian copyright exceptions are mandatory - then the option to mandate should also be mandatory. In all the other European Member States however, copyright exceptions are not mandatory. Contractual clauses can simply overwrite them. This implies that when a customer has signed a contract limiting the private copy exception by prohibiting the technical assistance of a third party service provider in making the copy, this customer will face contractual liability when using a DCR. The DCR-service provider faces a risk of being held liable for assisting the customer in breaching the contract with his television provider.

Apart from contractual restrictions, making copies can also be restricted by digital rights management systems (DRM). Digicorders, for example, often only allow a limited number of recordings at the same time or have limited hard disk storage. If such systems would be qualified as a DRM-system in the sense of the Copyright Directive, this could create additional risks for a DCR-service provider to roll out its business. After all, the Copyright Directive protects DRM systems by allowing national legislation to condemn the circumvention of such DRM systems[10]. In Belgium such perpetrators even face criminal prosecution. However, because of a somewhat unusual implementation of the Directive into Belgian law, circumvention could be qualified as legal if it serves a legitimate use[11]. Making a private copy could be qualified as such a legitimate use[12]. This creates an ambiguous situation in the sense that users who manage to work around DRM protection autonomously, in order to make a private copy are allowed to do so, but users who cannot, are not allowed to ask the television provider to take down the DRM for this legitimate use. After all, the BCA contains an article that instructs the party who implemented the DRM to take it down as a «voluntary measure», but only for specific exceptions. The exception for private copying was not taken up in that list…

Fourthly, a private copy can be made «on any medium». This clearly implies digital carriers such as external hard disks. In our opinion; storage «in the cloud», via remote servers, also falls within this scope. The fact that the physical medium upon which the copy was made and stored is not located in the customer's living room is in our view irrelevant since it is not required by the copyright exception.

---

10 Art. 6 and 7 Copyright Directive

11 Art. 79bis and 79terBCA

12 Amendement nr. 142 van Ms. Déom e.a., wetsvoorstel ter implementatie van de Copyright Directive, 17 mei 2004, *Parl. St.* Kamer 2003 – 2004, nr. 1137/012

If a private copy exception has been introduced in national law, the Copyright Directive stipulates that a system of fair compensation should be put in place to remunerate the right holders[13]. Belgian legislation provides for such a fair compensation system. The regulation, applicable to both recording devices and blanket media, was recently brought up-to-date. External hard disks, MP3 players, smartphones and set-top-boxes are new media that now can be charged with a fair compensation for private copying, paid by importers, producers and distributors of such devices to an overarching copyright society: Auvibel[14]. In essence, when the customer receives a digital digicorder device from their television provider, they automatically pay a fair compensation for their private copying since the television providers recover the cost of the compensation that they have to pay to Auvibel via their subscription fee and the renting (or sale) of the digicorder as a part thereof. Even when the customer does not use the device to make private copies, but would for example use a DCR instead, they are ultimately still paying. Admittedly, this is an indirect way of providing the necessary fair compensation. When a digital television provider however allows the customer to hold a subscription without renting/buying a digibox, a fair compensation will not be recovered by the provider through the customer. At the moment, virtual storage capacity in the cloud does not fall within the scope of the Belgian regulation for the fair compensation of private copying.

In our opinion, the non-existence of such a direct fair remuneration should not bar cloud service providers from developing DCR-applications. The Copyright Directive imposes this obligation to create and duly update a fair compensation mechanism for the right holders onto the Member States. Its existence and applicability is not the responsibility of service providers. The fact that the mechanism is not updated in a timely manner, notably in accordance with technological evolution, can therefore not be held against service providers enabling new ways of private copying which meet the customer's needs and which are otherwise not contrary to copyright law.

Finally, the specific conditions of the exception for private copying should be complemented by the more general conditions of the European «three-step-test»[15]. Since the implementation of the Copyright Directive, copyright exceptions only apply «*in certain special cases* [such as private copying] *which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the right holder*». There is much discussion amongst European scholars about the correct interpretation of the «three-step-test». A restrictive interpretation of this European «fair use»-system considers these conditions as being *additional* conditions and therefore as a «final check»

13 Art. 5.2 (b) Copyright Directive

14 Art. 55 - 58 BCA, juncto KB 17 december 2009 tot wijziging van het koninklijk besluit van 28 maart 1996 betreffende het recht op vergoeding voor het kopiëren voor eigen gebruik voor de auteurs, de uitvoerende kunstenaars en de producenten van fonogrammen en van audiovisuele werken, *B.S.* 23 december 2009.

15 Art. 5.5 Copyright Directive

when assessing the balance between users and right holders[16]. Although the goal of a DCR is clearly to expand the customers' possibilities within the realm of the private copy exception, we do not believe this expansion would conflict with a normal exploitation or would unreasonably prejudice the legitimate interest of the right holders. A DCR will not create a significant loss of income for right holders if the functionalities of the DCR are construed in a way that would enable them to pass the three-step-test. Possible ways of reaching this balance between interests of right holders and users are for example limiting the period of time a recording can be stored in the user's personal cloud (e.g. only 30 days) and/or limiting the amount of times a recorded program can be viewed (e.g. only once). Moreover, advertisements accompanying or inserted in the original broadcast should remain unaltered and the service provider should not give users the option to fast-forward them. In other words, this source of income for broadcasters should remain untouched. Finally, if the use of a digicorder is automatically or obligatorily included in the subscription to the television provider (which is often the case), a fair compensation will already have been paid by the subscriber to the right holders (if the relevant regulations have been updated up to this technological point). Additionally we should mention that an increasing amount of scholars is in favor of an «evolutionary interpretation» of the three-step-test[17]. Such an interpretation allows for a less restrictive approach in assessing the existing exceptions, taking into account technological evolutions. Some European judges already applied this interpretation in concrete cases[18]. This interpretation allows the extension of the scope of the private copy exception to encompass DCR-systems.

3.2. Exception for «temporary technical copies» as a safety net?

Our analysis of the exception for private copying only remains relevant in case the customer, and not the DCR service provider, qualifies as the «copier». In a French court case concerning the previously described Wizzgo application[19], the courts identified the

16 Conclusion Advocate-Generaal Trstenjak (2009). C-5/08, *Infopaq v. DDF. E.C.D.R.* 16 § 132.

17 Torremans, P. (2010). Archiving exceptions: where are we and where do we need to go. In Derclaye, E. (ed.). *Copyright and Cultural Heritage – Preservation and access to works in a digital world* (pp.124 etc.).Cheltenham: Edward Elgar Publishing; Senftleben, M.R.F. (2004). *Copyright, Limitations and the Three-Step-Test – an Analysis of the Three-Step-Test in International and EC Copyright Law.* Dordrecht: Kluwer Law International; Geiger, C. Griffiths, J. Hilty, R.M. (2008). Towards a balanced interpretation of the «three-step test» in copyright law (pp. 489-496). *European Intellectual Property Review*; Geiger, C. Griffiths, J. Hilty, R. M. Suthersanen, U. (2008). Déclaration en vue d'une interpretation du «test des trois étapes» respectant les équilibres du droit d'auteur (pp. 516-520). *A.M.* 2008/6. The original version in English of this Declaration can be retrieved from http://www.ip.mpg.de/shared/data/pdf/declaration_three_steps.pdf

18 Case I ZR 118/96, Bundesgerichtshof. 25 February 1999. *Juristenzeitung* 1999. 1000, note Schack, H.; Case I ZR 255/00 Bundesgerichtshof. 11 July 2002. *Juristenzeitung* 2003. 473, note Dreier, T.

19 T.G.I Paris, ordonnance de référé, 6 August 2008, *M6 Web et autres c. Wizzgo* and T.G.I. Paris (3e ch. 1er. Sect), 25 November 2008.

DCR-provider as the maker of the copy, not only in a technical sense, but also in a legal sense. If the service provider would be identified as the «copier», the exception for private copying cannot apply. Therefore we examined, in secondary order, whether the exception for «temporary technical copies» could be invoked by service providers. The exception for «temporary technical copies» is the only exception in the closed list of exceptions of the Copyright Directive which was obligatory and had to be implemented by all the European Member States[20]. Therefore we can find this exception in (almost) identical wordings in all European countries, also in Belgium.

However, if a DCR-service provider were to be qualified as the «copier», this exception would probably not apply. An act of reproduction under this exception is exempted from prior consent of the right holders if it meets five cumulative conditions. The copy should be (1) temporary, (2) transient or incidental, (3) an integral and essential part of a technological process, (4) its sole purpose should be to enable a transmission in a network between third parties by an intermediary, or a lawful use, of a work or other subject –matter and (5) should not have independent economic significance.

Although the exact scope of these conditions has been the subject of different questions asked to the European Court of Justice[21], much uncertainty remains. Concerning conditions (4) and (5), the recent decision of the court in *Football Association Premier League v. QC Leisure* clarified a few things. With regards to condition (5) the Court stated for example that «*independent economic significance*» should be interpreted as «*additional economic advantage going beyond the advantage derived from mere reception of the broadcasts at issue*». In other words: the technical copy must entail a financial return in addition to the financial return of the service itself. Soon the European Court will have the opportunity to confirm this interpretation in the British TV Catchup case[22]. As mentioned before TV Catchup does not provide a time-shifting function.

Regarding a DCR *with* time-shifting application, things are rather clear. Although the technical backbone of such a DCR undoubtedly generates multiple copies which could qualify as temporary technical copies in the sense of the corresponding exception (for example in case of simulcasting and other types of buffering between servers), the most important copy in the process is the full copy of an original broadcast which is *stored* in the cloud. It is clear that this copy will never meet conditions (1) (temporary) and (2) (transient and incidental). In other words: in case a service provider offering such a DCR-service would qualify as «the copier», no copyright exception could be invoked to exempt their use from the exclusive right of reproduction of the right holders. Prior consent of those right holders will be necessary for the acts of reproduction.

---

20 Art. 5.1. Copyright Directive

21 ECJ, 16 July 2009, *Infopaq v. DDF,* C-5/08; ECJ, 4 October 2011, *Football Association Premier League v. QC Leisure,* joined cases C-403/08 and C-429/08.

22 OUT-LAW News (2011). High Court asks ECJ if streaming service breaks copyright laws. Retrieved March 16th 2012 from http://www.out-law.com/page-12096

3.3. Does the use of the DCR imply a public or a private communication?

A DCR-service implies one or more acts of communication. Acts of communication could be identified in the upload of the broadcasted content into the servers («cloud»), the simulcasting of the content to the service provider's customers and the time-shifted unicasting of recorded content from the (private) cloud to the individual customers. The question will be whether these acts of communication qualify as a public communication or as a private communication. The relevance of the difference between the two can hardly be underestimated: a public communication is an exclusive right of the right holders which requires their prior consent; a private communication is not and can be done without a prior consent. The assessment of the acts of communication within a DCR is entangled with the previous analysis concerning the acts of reproduction and private copying. Depending on the outcome of the previous issues, we can describe two scenarios.

3.3.1. Scenario 1: Customer is «copier» and playback of copy is a «private communication»

In this scenario we assume that the recording was made by the customer under the private copy exception. In this hypothesis the communication in question would be a stream of that private copy of the customer to himself. This playback feature cannot be qualified as a public communication: the customer simply «consumes» their privately made recording. The playback feature is a necessary completion of the private copy. Furthermore, Belgium has a specific copyright exception for «private performance», i.e. performances within the privacy of the «family circle». In fact, those exceptions are rather peculiar, since they delineate the exclusive communication right which only comes into play when it concerns a communication to the public.

In the TVNow case, the Australian judge mentioned the fact that the customer had to press the «play» button on the TVNow-interface as an indication that he initialized the communication to himself of a recording he made earlier. The judge compared this with the use of a recording on a VHS cassette, which is inserted into the VHS player and put in motion by pressing the «play» button. Any DCR-technology would require the customer to undertake a similar action, namely to press some kind of a ''play» button in order to launch his video stream. In our opinion this system will qualify as a private communication within this scenario, since it will only be the individual customer who has access to his own content and given the fact that he watches the content within his own private «family circle».[23]

In this scenario the only potential risk for a DCR-service provider that remains, is to be found in the technology used to redistribute the recorded content. If this extra feature would be enabled by uploading the content by the customers into a peer-to-peer

23 Importance of the fact that only individual customers have access to the service has been confirmed by the national judges in both the TVCatchup case (*ITV Broadcasting a.o. v. TV Catchup*, High Court of Justice, 18 July 2011, Case n° HC10C01057, London) and the Cablevision case (*Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d121 (Court of Appeal, 2d Cir.), 4 August 2008).

network in which everybody shares parts of the same broadcast, the uploading-action and following sharing (redistribution) amongst peers will almost certainly qualify as a public communication, executed by the users of the DCR (since they make the recording). It seems inadvisable from a business point of view to potentially incriminate your own customers by providing them a technology that forces them to unintentionally communicate audiovisual protected content to «the public» (the peer-to-peer network). On the other hand, some peer-to-peer technologies are not illegal per se and are increasingly put forward as a way to efficiently store content in the cloud[24]. The outcome of this issue before any given court is highly unpredictable.

3.3.2. Scenario 2: Service provider is «copier» and playback feature is a «communication to the public»

If not the customer but the service provider would be identified as the «copier», it seems logical that they will also be identified as the party initiating the communication to the customers. The question that remains is whether or not the acts of communication in this scenario are public or not.

The exclusive right of public communication is interpreted in a broad way. Every communication which can be received by an audience, even if this audience is not present at one place or watching at the same time, qualifies as a public communication. With regard to technical intermediaries, art. 11bis of the Berne Convention, art. 3 Copyright Directive and the Satcab Directive[25] institutionalize this broad interpretation for transmission by technical means (such as satellite, cable or otherwise). In light of art. 11bis Berne Convention, every transmission of programs with or without «a wire», by intervention of another organization than the original broadcaster, falls within the scope of the public communication right, even if this intervention is purely passive. The public character of the communication should be assessed at the moment of transmission by the intermediary organization and not at the moment of reception by the customer. This interpretation by a Belgian judge[26] could definitely apply to a DCR-service provider. With regard to the simulcast modus, this could even qualify as a «cable retransmission» under the Satcab regime, if this simulcast would be «live» or «near-live» and would not alter the original broadcast (for example by removing, changing or inserting commercials).

In the same judgment, the judge states that it is irrelevant whether or not the intervening organization targets a new audience or not. Even if the same audience of the original broadcast is targeted, the communication would still qualify as a public communication or

24 See for example the MP3tunes-case (USA), *Capital Records Inc et al v. MP3tunes LLC et al*, U.S. District Court, Southern District of New York, No. 07-09931

25 Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, *O.J.* no. L346 of 1992-11-27, p. 61.

26 Cass. 3 September 1981, *Pas.* 1982, I, 8 ; ECJ. 18 March 1980, Coditel I, C-62/79, *Jur.* 1980, I-881.

a retransmission. The High Court of the Netherlands decided likewise in a similar case[27]. Nonetheless, European jurisprudence states that it *is* relevant to assess whether or not a *new* public is being reached in order to qualify the communication as being public[28]. In its Premier League-decision, the European Court clearly points out that «*in order for there to be a 'communication to the public' within the meaning of Article 3(1) of the Copyright Directive* [aka Infosoc Directive] *[…] it is also necessary for the work broadcast to be transmitted to a new public, that is to say, to a public which was not taken into account by the authors of the protected works when they authorized their use by the communication to the original public […]. When those authors authorize a broadcast of their works, they consider, in principle, only the owners of television sets who, either personally or within their own private or family circles, receive the signal and follow the broadcasts.* [highlighting by authors]*»*. This additional condition for a communication to be qualified as public could in any case render the simulcast modus of a DCR-service a private communication, since no new audience is being targeted. After all, such a simulcast only serves customers who subscribed to a digital television provider and only streams the content to those who are in any case entitled to receive it. Again, the upcoming TV Catchup decision of the European Court will soon have to provide an answer.

With regard to a DCR with time-shifting modus it is difficult to make a prediction. The playback of a recording will probably not qualify as a public communication by cable retransmission, since the retransmission does not take place at the same time as the original broadcast. The playback of the DCR could however easily qualify as a public communication in the sense of art.3 Copyright Directive, since this article clearly states that a communication is public if the public has access to it at a time individually chosen by them. We could however imagine that the extra condition (*new* audience) introduced by the European Court applies to art. 3 Copyright Directive *in general*, and not only in the particular case of simulcasting. Since a DCR can mostly only be used by subscribers paying to a television provider, no new audience will be targeted by the DCR-service provider, which would render the communication –again- not public. However, both the Premier League case and the TV Catchup case deal with simulcast-streaming (in spite of the latter's name) and not with playback of recorded content. To conclude, it remains to be seen how the European Court would qualify the business model of a «full option» DCR in terms of copyright and related rights.

4. CONCLUSION

The above analysis shows that the actual Belgian and European copyright framework do not offer straight-forward answers to all the legal questions one can ask regarding a «full-

27 Hoge Raad 30 October 1981, *NJ* 1982, 435, and final decision after referral: Hoge Raad 25 May 1984, *NJ* 1984, 697

28 ECJ, Conclusion of Advocate-General Jääskinen, N., 17 March 2011, *Airfield and Canal Digitaal v. Sabam*, joined cases nr. C-431/09 and nr. C-432/09 and ECJ, 4 October 2011, *Football Association Premier League v. QC Leisure,* joined cases C-403/08 and C-429/08

option» DCR. A vast margin for interpretation, restrictive or evolutionary, still remains with regard to the most relevant issues: Who is the copier? What with general contractual clauses? Can you circumvent DRM? Is there a communication to the public? Etc.) which creates legal uncertainty for all stakeholders at hand: cloud service providers, consumers and right holders. The different court decision of the ECJ are –step by step- trying to harmonize some of these answers, although until now always in cases related to audiovisual content, but not directly on the kind of DCR-services we are assessing. The upcoming TVCatchup decision will no doubt offer some welcome answers, yet we would need a TVNow-type case in order to receive the answers that could create a risk-free environment for DCR-services to be marketed. Therefore, however, one DCR-service provider would have to take the risk to launch such a service without those clear answers…and go all the way to obtain them.

5. BIBLIOGRAPHY

Senftleben, M.R.F. (2004). *Copyright, Limitations and the Three-Step-Test – an Analysis of the Three-Step-Test in International and EC Copyright Law.* Dordrecht: Kluwer Law International;

Brison, F. Vanhees, H. (eds.) (2008). Huldeboek Jan Corbet – De Belgische Auteurswet, Artikelsgewijze commentaar. Gent: Larcier;

Geiger, C. Griffiths, J. Hilty (2008). Towards a balanced interpretation of the «three-step test» in copyright law. *European Intellectual Property Review*;

Geiger, C. Griffiths, J. Hilty, R. M. Suthersanen, U. (2008). Déclaration en vue d'une interpretation du «test des trois étapes» respectant les équilibres du droit d'auteur. *A.M.* 2008/6;

Stamos, T. (2009). La copie privée cherche à s' étendre: feu vert pour le vPVR?. *Revue du droit des technologies de l'information. 36.* 105-128;

Standeford, D. (2009). US Cablevision Decision Has Implications For Cloud Computing, Online Advertising. *Intellectual Property Watch.* 3 July 2009. Retrieved March 22th 2012 from http://www.ip-watch.org/2009/07/03/us-cablevision-decision-has-implications-for-cloud-computing-online-advertising/

Singapore Keystone Law Alert (2010). [2010 Edition Issue 11A of 30 November 2010 contains an entry (without title) on a DCR-case in Singapore, RecordTV]. Retrieved March 22th 2012 from http://www.keystonelawcorp.com/downloads/SingaporeKeystoneLaw2010-11A.pdf

Torremans, P. (2010). Archiving exceptions: where are we and where do we need to go. In Derclaye, E. (ed.). *Copyright and Cultural Heritage – Preservation and access to works in a digital world.* Cheltenham: Edward Elgar Publishing;

OUT-LAW News (2011). High Court asks ECJ if streaming service breaks copyright laws. Retrieved March 16th 2012 from http://www.out-law.com/page-12096

Smith, J. Mallam, M. (2011). TV catchup paused as High Court refers to Europe, *JIPLP Weblog.* 8 November 2011. Retrieved March 22th 2012 from http://jiplp.oxfordjournals.org/content/6/12/860.full

GUIDING PRINCIPLES FOR ONLINE COPYRIGHT ENFORCEMENT

Andrew McDiarmid
Senior Policy Analyst
David Sohn
General Counsel
Center for Democracy & Technology

ABSTRACT: Copyright applies no less online than off, and there is no inherent conflict between copyright protection and enforcement on one hand and innovation and human rights on the other. Nonetheless, the means chosen to enforce copyright matter a great deal. Some tactics could be attractive to rightsholders, but would carry significant costs to innovation, free expression, privacy, and other important interests. So that policymakers can avoid these risks, this paper puts forward six principles to guide online copyright policymaking:

1. Maintain a narrow focus on bad actors.
2. Avoid abandoning longstanding and successful existing policies and imposing intrusive new network-policing roles on intermediaries.
3. Soberly assess a policy's likely effectiveness and collateral impacts on legitimate entities and human rights.
4. Voluntary efforts between rightsholders and intermediaries can be effective, but must be developed in a manner that ensures that the public interest is strongly represented and protected.
5. Set a realistic goal: making participating in widespread infringement unattractive and risky compared to participating in lawful markets.
6. Enforcement alone will not be effective; increased availability of compelling legal options for obtaining copyrighted works and public education about the consequences of infringement are both essential to reducing infringement.

The paper then applies these principles in a case-study analysis of recent efforts to use the Domain Name System to target websites devoted to infringement, demonstrating the shortcomings of those tactics.

KEYWORDS: Copyright enforcement, free expression, Internet intermediaries, domain names, DNS, Stop Online Piracy Act (SOPA), PROTECT IP Act (PIPA).

1. INTRODUCTION

Online copyright policy must strike a balance that respects and provides for the enforcement of the rights of content creators without curtailing the Internet's tremendous potential for fostering innovation and free expression. Copyright applies no less online than off, and there is no inherent conflict between copyright protection and enforcement on one

hand and Internet innovation on the other. Indeed, both Internet openness and respect for copyright can promote and enable innovation and expressive activity.[1]

There is no substitute for fair and targeted enforcement against those who infringe copyrights or actively encourage infringement. At the same time, copyright enforcement must not target technologies or providers of multipurpose online services, both because of the risk of stifling lawful content and because of the chilling effect enforcement against intermediaries would have on the development of beneficial services. New digital and Internet-based media and communications tools are of great value to consumers, the economy, and society in general.

In finding the right balance, the *means* chosen to enforce copyright online matter a great deal. Some potential tactics could be attractive from a copyright protection perspective, but would carry significant costs to innovation. Recent proposed legislation in the United States, for example, which called for new enforcement measures against websites dedicated to infringement, faced great popular opposition and was ultimately withdrawn. The opposition was due in large part to the overbroad and damaging impact certain tactics included in the legislation would have had on legitimate expression and lawful online services.

This paper offers six principles for policymakers as they consider measures to address online copyright infringement. The paper then applies several of these principles to illustrate the shortcomings of domain-name seizure and blocking – the former of which is currently practiced by U.S. law enforcement, and the latter of which was included among the proposals in the withdrawn U.S. legislation.

2. PRINCIPLES FOR ONLINE COPYRIGHT ENFORCEMENT

2.1. Copyright enforcement should target true bad actors. Ratcheting up copyright protections across the board would impair legitimate business activity and chill technological innovation that drives free expression

It is easy to think of copyright enforcement as simply a question of catching and punishing bad actors. There is indeed a great deal of straightforward infringement online – practices that are clearly illegal, and pirate enterprises that are clearly culpable. If this were the only kind of activity affected, there would be little downside to efforts to ratchet up copyright enforcement and remedies.

In practice, however, copyright enforcement in the information age affects a wide range of entities and behaviors. In a digital economy, many common activities and many well-intentioned parties can face difficult and contentious copyright challenges. There are many gray areas, and maintaining focus on true bad actors is not always easy. Any time a consumer forwards an email, moves content from one device to another, or uses digital tools to create

1 *See* Center for Democracy & Technology (2010). *Protecting Copyright and Internet Values: A Balanced Path Forward*. Retrieved March 26, 2012 from http://www.cdt.org/copyright/20050607framing.pdf.

content, it can raise copyright questions.[2] The legal boundaries separating lawful and unlawful activity often are not clear, especially when content may implicate fair use or other limitations and exceptions to copyright protection.

The challenges facing innovators in the Internet and information technology sectors are particularly acute. In today's world, all kinds of devices and services boast computing power, memory, and network connectivity. They enable users to store, transmit, and manipulate data in new ways. Inevitably, they make copies or enable users to do so. Many services rely on copyright exceptions and limitations to function, and they often raise novel questions of copyright law.[3] Those questions lead to business disputes and lawsuits.

It is essential for policymakers to recognize, therefore, that copyright law and enforcement practices can implicate legitimate innovative companies, not just pirate enterprises. Strong copyright enforcement tools, such as injunctions or high monetary damages, are often brandished against upstart companies in business disputes. Strengthening such tools can significantly increase the leverage of copyright interests in negotiating and trying to obtain settlements, even where is it highly unclear that the law is on their side.

The concern that copyright enforcement can affect innovative businesses operating in good faith is by no means theoretical. Technologies that have been targeted in copyright disputes in the U.S. include the following:

- **VCRs.** Movie studios famously sued Sony, the maker of the Betamax VCR, for providing users with the ability to record copyrighted television programs. Outcome: The U.S. Supreme Court held in 1984 that non-commercial copying for private «time-shifting» is a fair use and that Sony was not liable for the potential infringing behavior of some users.[4] The home video market subsequently grew into a major source of revenue for the entertainment industry.
- **Network-Based Digital Video Recorders.** Owners of cable television programming sued Cablevision for proposing to offer a digital video recorder – the digital equivalent of a VCR – that would record programs on a central server instead of on a device in the user's home. Outcome: A 2007 court ruling stalled the technology by finding it to violate copyright; a year-and-a-half later, an appeals court reversed, finding no copyright infringement.[5]
- **Family-Friendly DVD Players.** Film directors sued a company that marketed a DVD player designed to skip portions of movies containing sexual or violent content, as

2 *See* Tehranian, John (2007). Infringement Nation: Copyright Reform and the Law/Norm Gap. In Utah Law Review 537. http://ssrn.com/abstract=1029151.

3 CCIA (2011). *Fair Use in the U.S. Economy: Economic Contributions of Industries Relying on Fair Use*. Retrieved March 25, 2012 from http://www.ccianet.org/CCIA/files/ccLibraryFiles/Filename/000000000526/CCIA-FairUseintheUSEconomy-2011.pdf.

4 *Sony Corp. of America v. Universal City Studios, Inc.* 464 U.S. 417 (1984).

5 *The Cartoon Network LP, et al., v. CSC Holdings, Inc. and Cablevision Sys. Corp.* 536 F.3d 121 (2d Cir. 2008), *cert. denied* 129 S. Ct. 2890.

well as a company that edited and redistributed lawfully purchased DVDs to achieve the same result. Outcome: Congress stepped in to give family-friendly DVD players a legislative exemption.[6] The company making edited DVDs, however, was ruled to infringe.[7]

- **Portable mp3 Players.** The recording industry sued Diamond, Inc., the maker of an early portable mp3 player, arguing that it was required to include copy-protection technology specified in the U.S. Audio Home Recording Act. Outcome: The Ninth Circuit Court of Appeals ultimately ruled that devices with multi-purpose computer hard drives were not covered,[8] paving the way for iPods and the rest of the now-booming digital music player industry.
- **Search Engines for Images.** Perfect 10, an adult entertainment company, sued Amazon, Google, and Microsoft for providing online search engines that index and display thumbnail versions of images they find posted on third-party websites. A photographer sued an early, smaller provider of image search as well. Outcome: After extensive litigation, the Ninth Circuit Court of Appeals held that the copying and display necessary to operate image search engines constitutes fair use.[9]
- **Full-Text Search for Books.** Major publishers sued Google for its Book Search project, which initially involved scanning books into an index to enable a full-text search engine. Outcome: The court rejected a proposed agreement to settle the case and litigation is ongoing.[10]
- **Video-Sharing Websites.** In 2007, Viacom filed a blockbuster lawsuit against YouTube, demanding $1 billion in damages based on infringing videos uploaded by YouTube users. Other video-sharing sites that have been sued on similar grounds include Veoh,[11] MySpace,[12] VideoEgg,[13] Grouper,[14] and Bolt.[15] Outcome: While some cases have been settled, the YouTube litigation is ongoing. A recent appellate decision in the YouTube case resolved some of the key legal questions in a manner largely favorable to YouTube, but sent the case back to a lower court to consider some remaining factual questions.[16]

---

6 Family Home Movie Act of 2005. U.S. Pub. L. no. 109-9 (2005) § 110(11).

7 *Clean Flicks of Colo., LLC v. Soderbergh*. 433 F. Supp. 2d 1236 (D. Colo. 2006).

8 *RIAA v. Diamond Multimedia Systems, Inc.* 180 F.3d 1072 (9th Cir. 1999).

9 *Perfect 10, Inc. v. Amazon.com, Inc.* 508 F.3d 1146 (9th Cir. 2007); *Kelly v. Arriba Soft Corporation*. 336 F.3d 811 (9th Cir. 2003).

10 *The Authors Guild, et. al., v. Google, Inc.* 05 CV-8136 (DC) (S.D.N.Y 2005).

11 *UMG Recordings, Inc. v. Shelter Capital Partners LLC* 2011 WL 6357788 (9th Cir. Dec. 20, 2011).

12 *UMG Recordings, Inc. v. MySpace, Inc.* CV 06-7361 AHM (AJWx) (C.D. Cal. 2008).

13 *Capitol Records, LLC., et. al. v. VideoEgg.* 08 CV-5831 (S.D.N.Y. 2008).

14 *UMG Recordings, Inc. v. Grouper, Inc.* CV 06-06561 (C.D. Ca. 2006).

15 *UMG Recordings, Inc., et al. v. Bolt, Inc., et. al.* CV 06-06577 (C.D. Cal. 2006).

16 *Viacom Int'l, Inc., v. YouTube, Inc.* 10-3270-cv, 2012 WL 1130851 (2nd Cir. April 5, 2012).

Veoh won a similar appeal, although the costs of litigation caused the site to go out of business in the process.[17] Without safe-harbor protection, user-generated content sites likely could not exist in anything like their current form.

- **Auction Sites.** Tiffany and Co. brought trademark claims against eBay for the sale by users of counterfeit Tiffany goods through the auction website. Outcome: In a ruling with significant implications for online auctions and e-commerce, an appeals court upheld a lower court's dismissal of all trademark claims.[18] A finding of liability would have placed a tremendous burden on these services, constraining their ability to operate.
- **Cell Phone Ringtones.** The American Society of Composers and Publishers (ASCAP) sought performance royalties from wireless phone companies for the ringtones that play when users' phones ring. Outcome: A court declined to hold wireless companies liable for royalties every time a user's ringtone rings in public.[19]
- **Garage-Door Remote Controllers.** A maker of garage-door openers sued a maker of a universal remote controller, alleging unlawful circumvention of a technological protection measure protecting the code that operated the garage-door opener. Outcome: After years of litigation, a court rejected this claim.[20]
- **Replacement Printer Cartridges.** Lexmark, a printer manufacturer, sued a maker of replacement ink cartridges for circumventing computer code designed to bar the use of non-Lexmark cartridges. Outcome: A lower court ruled in favor of Lexmark, but the Sixth Circuit Court of Appeals eventually overturned that ruling.[21]
- **Computer Equipment Maintenance Services.** StorageTek, a maker of digital storage equipment, argued that an independent company providing maintenance services for StorageTek equipment unlawfully circumvented technological protections restricting access to the software controlling the equipment. Outcome: A court found no violation because the circumvention was not connected to any act of infringement.[22]

The point here is not that copyright disputes involving new technologies always should be resolved in favor of the technology providers and against the copyright holders. Reasonable people can and do disagree about the optimal legal outcomes from case to case. But it should be clear that mechanisms for enforcing copyright are often brought to bear against technologies that may well be lawful, resulting in substantial uncertainty and delay in the rollout of new or competitive products and services.

---

17 Kafka, Peter (February 11, 2010). «Veoh finally calls it quits: Layoffs yesterday, bankruptcy filing soon.» *CNet*. Retrieved March 26, 2012 from http://news.cnet.com/8301-1023_3-10452152-93.html.

18 *Tiffany Inc. v. eBay, Inc.* 600 F.3d 93 (2nd Cir. 2010).

19 *U.S. v. ASCAP (In re Application of Cellco Partnership d/b/a/ Verizon Wireless).* 663 F. Supp. 2d 363 (S.D.N.Y 2009).

20 *Chamberlain Group, Inc. v. Skylink Technologies, Inc.* 381 F.3d 1178 (Fed. Cir. 2004).

21 *Lexmark International, Inc. v. Static Control Components, Inc.* 387 F.3d 522 (6th Cir. 2004).

22 *Storage Tek v. Custom Hardware.* 421 F.3d 1307 (Fed. Cir. 2005).

The key lesson is that when and whether copyright liability should extend beyond individual infringers to the providers of technology and services is a highly complicated issue with major implications not just for copyright holders, but for multiple sectors of the economy and for the public. Law and policy in this area should be careful to keep a narrow focus on bad actors and avoid creating legal landmines for legitimate businesses.

Any new copyright enforcement policies, therefore, should include measures to protect legitimate companies from being subject to the same tough enforcement tools as true piracy rings. Indeed, the litigation risks that copyright law imposes on legitimate businesses is already a significant problem. In the digital age of cheap and rapid copying, statutory damages can quickly reach astronomical levels that could break the backs of most companies.[23] A company that believes with 98 percent certainty that its activity is lawful (that it falls within fair use, for example) still needs to consider whether it would be wise to take a two percent risk of bankrupting the company.

Thus, copyright law can chill innovation, and further changes to expand or strengthen enforcement tools could exacerbate the problem. As any new enforcement tactic is considered, policymakers must take careful account of the possible impact on legitimate services that drive innovation, commerce, and free expression.

2.2. Existing policies establishing safe harbors for Internet intermediaries have been tremendously successful. Policymakers should avoid abandoning those policies in favor of imposing new network-policing roles on intermediaries

It is longstanding policy in the U.S., Europe, and elsewhere that Internet intermediaries such as websites, hosting services, and Internet service providers (ISPs) generally should not be liable for content created by their users.[24] In section 230 of the Communications Act and section 512 of the Digital Millennium Copyright Act (DMCA), the U.S. Congress provided important statutory safe harbors from intermediary liability for third-party content.[25] The 2001 E.U. E-Commerce Directive provides similar protections.[26] In the U.S. courts, the landmark 1984 case involving the Sony Betamax VCR established the principle that making and distributing a product does not give rise to liability for infringements users may commit with that product, so long as the product is «capable of substantial noninfringing use.»[27] The 2005 *Grokster* decision reaffirmed the «substantial noninfringing use» test: taking active

23 In the U.S., pre-set statutory damages range from $750 to $150,000 per work infringed. *See* 17 U.S.C. § 504(c)(1).

24 *See* WIPO (2011), *Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries (Preliminary Version)*. Retrieved March 23, 2012, from http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries.pdf.

25 47 U.S.C. § 230(c)(1); 17 U.S.C. § 512.

26 European Union Directive 2000/31/EC. Available at http://ec.europa.eu/internal_market/e-commerce/directive_en.htm.

27 *Sony v. Universal* 464 U.S. 417 (1984), *supra* note 4.

steps to promote and encourage infringement can give rise to liability, but the mere act of distributing a multipurpose product does not – even if the product's maker knows that some infringing uses are certain to occur.[28]

These policy choices have been nothing short of a tremendous success. It is thanks to this legal framework that recent decades have seen an explosion of innovation in digital technologies and Internet-based products and services. Protection from potentially ruinous copyright liability risk has created an innovation environment in which technology providers can focus on developing tools that empower users and companies can grow from small start-ups to household names with unprecedented speed.[29] Society benefits from the current innovation-friendly legal framework in the form of increased opportunities for speech, collaboration, civic engagement, and economic growth.

Protections from liability have been particularly essential in enabling interactive and user-generated content sites to flourish. If ISPs, hosts, and websites with no bad intent were instead made potentially liable for content posted by others, they would have no choice but to assume new gatekeeper roles and pare back functions that empower communication by and among users. Entry barriers for new Internet services (including new competitors to existing services) would increase substantially, the Internet's openness to innovation would be reduced, and service providers would be reluctant to host controversial but lawful speech.

The same risks arise from approaches that seek to directly impose enforcement obligations on Internet-based service providers, as opposed to holding them liable for infringement. Raising enforcement burdens on intermediaries can impose new costs that can alter the incentives for investing in and launching new services.[30]

Imposing policing obligations on ISPs in particular also risks setting a dangerous global precedent for Internet freedom. The tools used to carry out such obligations are the same tools used in some cases to carry out invasive surveillance and political censorship. Therefore, requiring their adoption risks legitimizing the use of these tools, undermining advocacy against repressive practices. For the United States, resisting the adoption of these tools has become a major foreign-policy objective. Secretary of State Hillary Clinton has continually urged other countries to allow the provision of Internet access as an open communications platform without centralized supervision or monitoring.[31] CDT and others have argued that this advocacy would

28 *MGM Studios Inc. v. Grokster, Ltd.* 545 U.S. 913.

29 *See* Booz & Co. The Impact of U.S. Internet Copyright Regulations on Early-Stage Investment (2011). Retrieved April 30, 2012, from http://www.booz.com/media/uploads/BoozCo-Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf.

30 *See* Brad Burnham (March 13, 2012). «Freedom to Innovate» (Remarks at CDT Annual Dinner). Retrieved March 14, 2012, from http://www.usv.com/2012/03/the-freedom-to-innovate.php. (arguing that shortsighted regulations by the U.S. will push innovators and entrepreneurs to invest in countries outside the United States).

31 Secretary of State Hillary Rodham Clinton (January 21, 2010). Remarks on Internet Freedom, address at The Newseum. Retrieved from http://state.gov/secretary/rm/2010/01/135519.htm.

be undermined if the U.S. were to adopt tactics that authoritarian regimes could use to justify their own surveillance and censorship.[32] Policymakers must remain aware of the ways in which tools ostensibly adopted to combat copyright infringement can be misused in other contexts.

For all these reasons, policymakers should avoid the myopic approach of departing from well-established policy principles to impose new, affirmative network-policing obligations on Internet intermediaries.

2.3. Rigorous cost-benefit analysis is essential in evaluating new policy proposals for addressing online copyright infringement. There needs to be a sober assessment of a policy's likely effectiveness and its collateral impact on legitimate content and entities

Concern about copyright infringement is understandably high. Although there is good reason for skepticism in accepting major rightsholders' reports of the damage piracy does to their industry, there is general agreement that widespread infringement persists and has a significant impact on rightsholders' business.[33] This does not mean, however, that any and all proposals for reducing infringement are worthy of pursuit or government endorsement. As in any area of policy, proposals for new anti-infringement measures must be subject to rigorous cost-benefit analysis, asking both how effective a proposed policy is likely to be in reducing infringement and what negative collateral impact it may have.

Policymakers should be particularly alert to the risk that, where the benefits and costs of a measure accrue to different parties, it can be in the interest of the beneficiaries (likely the rightsholders) to lobby strongly even for a measure that offers relatively minor private gains at high social cost. Careful, independent consideration and balancing of the true costs and benefits of suggested measures is essential.

It is important that consideration of costs and benefits be made with a long view. Online copyright enforcement efforts are often characterized as an arms race, with determined infringers developing workarounds and new methods to infringe soon after new enforcement tactics take hold.[34] Consequently, many enforcement efforts may suffer from diminishing returns. At the same time, collateral damage to other policy objectives – such as protecting individuals' privacy or encouraging the global development of online platforms for speech and commerce – may be siginificant and long-lasting.

---

32 Statement of CDT before the Senate Judiciary Committee, Subcommittee on Human Rights and the Law: *Global Internet Freedom and the Rule of Law II* (March 2, 2010). 111th Congress, 2nd Sess. Available at http://www.cdt.org/files/pdfs/20100302_cdt_global_net_freedom.pdf.

33 U.S. Government Accountability Office (April 2010). *Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*. Retrieved March 26, 2012, from www.gao.gov/new.items/d10423.pdf. (stressing the difficulty in verifying industry estimates of piracy's impact, while acknowledging that infringement is a serious problem).

34 *See*, generally, Peter Biddle et. al. (Microsoft 2002). *The Darknet and the Future of Content Distribution*. Retrieved March 26, 2012, from http://msl1.mit.edu/ESD10/docs/darknet5.pdf.

In short, if a particular proposal's reduction in online infringement is likely to be of marginal size or fleeting duration and the proposal would impose significant burdens on (for example) legitimate innovators or online free expression, then the proposal should be rejected.

2.4. There may be opportunities for progress through voluntary, collaborative approaches that do not involve government mandates. Such approaches must, however, be developed in a manner that ensures that consumer and innovation interests are strongly represented and protected

Voluntary, collaborative efforts between copyright holders and other parties in the Internet ecosystem can make an impact on infringement levels. Voluntary efforts carry less risk to innovation, because by definition they do not burden innovators with one-size-fits-all mandates that might prove too costly, awkward to implement, or simply effective in some contexts. To the extent that they are truly voluntary, rather than the product of government demands or pressure, such private-sector efforts also avoid the constitutional questions (for example, due process, or inadvertent impact on lawful expression) that can arise when government action is involved. On the other hand, private deals by entities providing Internet services or online platforms can still have a substantial impact on their users. The lack of government involvement makes it all the more important that private parties working out voluntary arrangements take affirmative steps to ensure that the consumer and innovation interests of users are represented and protected as collaborative approaches are developed.

For example, major user-generated content sites have developed content-filtering tools to address uploads of copyrighted material.[35] From a user perspective, it is important that such filtering tools leave room for copyright's limitations and exceptions (e.g., fair use), operate transparently, and allow users the opportunity to object if they believe a filter has wrongly blocked a lawful posting. Interestingly, some voluntary filters help minimize the impact on users by encouraging revenue-sharing partnerships between user-generated content sites and rightsholders as an alternative to blocking unauthorized postings.[36] This approach offers the promise of moving beyond content blocking and legal battles to focus instead on building new markets. *Mandating* filtering tools, however, would likely stifle the development of such innovative licensing arrangements.

As another example, ISPs and content owners in the U.S. have announced an agreement to cooperate on a system of «escalating alerts» to suspected infringers.[37] While much

35 *See, e.g.*, YouTube's Content ID System at http://www.youtube.com/t/contentid.

36 In August 2008, YouTube reported that rightsholders chose to allow their content to be uploaded, sharing in ad revenue, 90 percent of the time. *See* Brian Stelter (August 15, 2008). Some Media Companies Choose to Profit From Pirated YouTube Clips. *New York Times*. Retrieved March 25, 2012, from http://www.nytimes.com/2008/08/16/technology/16tube.html?_r=1.

37 Memorandum of Understanding between U.S. copyright industries and ISPs (July 6, 2011). Retrieved March 26, 2012, from http://www.copyrightinformation.org/sites/default/files/Momorandum%20of%20Understanding.pdf.

depends on the details of how this system of notice-forwarding will be implemented,[38] it has the potential to reduce levels of peer-to-peer infringement. The notices will serve an educational purpose, making it clear that the subscribers' behavior is not as anonymous as they may have believed. In the case of families sharing a computer, a notice may alert the parents that a child is engaged in unlawful filesharing, which may prompt the parents to intervene. Given the possibility of serious penalties for infringement, warning notices may be quite effective in prompting recipients to cease infringement.[39]

Any attempt to move beyond warning notices to actual ISP-imposed sanctions, however, would implicate user rights in a much more fundamental way.[40] The Internet has become essential for many aspects of personal, professional, and civic life. Disabling or restricting subscribers' Internet access, even in a temporary or limited way, can have significant consequences. Any such sanctions would need to take great care in ensuring due process for subscribers, including the opportunities to answer allegations and to appeal or otherwise take some recourse in case sanctions are applied wrongfully. In addition, the process would need to include consideration of such factors as potential hardship, unintentional violations, and impact on innocent members of an affected household. Finally, there would be substantial questions about proportionality; permanent termination, for example, would be difficult if not impossible to justify.

In negotiating voluntary, cooperative agreements, private entities need to be sensitive to a range of public interests beyond just those of the copyright holders and Internet or online service providers in question. This can best be accomplished by seeking input and participation from persons or civil-society groups focused on representing those interests before any final deal is made.

2.5. Online copyright policy should set a realistic goal: making participation in widespread infringement relatively unattractive and risky, compared to participating in lawful markets

Eliminating copyright infringement completely is an impossible task. The goal of copyright policy needs to be more realistic: not to prevent infringement entirely, but rather to make it relatively unattractive and risky compared to participating in legal markets. Some

38 *See* David Sohn (July 7, 2011). ISPs and Copyright Owners Strike a Deal. *CDT Policy Beta blog*. Retrieved March 23, 2012, from https://www.cdt.org/blogs/david-sohn/isps-and-copyright-owners-strike-deal.

39 A 2007 Canadian study found notices effective at deterring infringement. *See* E-mail warnings deter Canadians from illegal file sharing. *CBC News* (February 15, 2007). Retrieved March 25, 2012, from http://www.cbc.ca/consumer/story/2007/02/14/software-warnings.html.

40 *See*, French Constitutional Council (June 10, 2009). Decision regarding the Law Promoting the Diffusion and Protection of Creativity on the Internet, Law No. 2009-669. Retrieved March 25, 2012, from http://www.conseil-constitutionnel.fr/decision.42666.html. (Striking portions of a «three strikes» law deemed inconsistent with the French constitution.)

people will no doubt continue to engage in large-scale infringement no matter what. The software industry, however, has managed to be quite profitable despite stubbornly high rates of infringement, demonstrating that a content business does not need to eliminate all illegal infringement in order to succeed.

Efforts to pursue a more ambitious goal – such as complete or near-complete elimination of large-scale infringement – would risk taking copyright policy in a harmful direction for innovation. Copying and disseminating data are core functions of computers and the Internet. Any law or policy aiming to curtail the *technical* capability of people to engage in copyright infringement, therefore, has to go down the radically dangerous path of restricting access to or hobbling the very technologies that are central to the information economy. In the computer and Internet age, there simply is no good policy option for making infringement technically infeasible.

Framing the goal in a realistic way should help clarify that policy initiatives in this area need not and should not target multipurpose technologies or multipurpose online services in a vain attempt to restrict the public's access to technological tools that have the potential to be employed for infringement. Rather, copyright enforcement efforts should focus on deterring and punishing the illegal *use* of digital technologies and services.

In that context, it is important to recognize that rightsholders already have a powerful set of copyright enforcement tools at their disposal. In the U.S., for example:

- Rightsholders can bring lawsuits against infringers.
- Rightsholders can bring secondary liability lawsuits against companies that actively induce infringement, following the Supreme Court's 2005 *Grokster* decision.[41]
- Rightsholders benefit from a generous statutory damages regime that allows them to recover from $750 to $150,000 per work infringed, without having to make any showing regarding actual damages suffered.[42] The threat of such statutory damages gives rightsholders considerable leverage in settlement or cease-and-desist discussions with actual or potential defendants.
- The «notice-and-takedown» regime created by section 512(c) of the DMCA enables rightsholders to demand the removal by online content hosts of any material the rightsholders identify as infringing.
- The anticircumvention provisions of section 1201 of the DMCA give the force of law to any technological protection measures that individual rightsholders choose to deploy.[43] Whenever a rights holder employs «digital rights management» technology to limit access to a copyrighted work – whatever form such DRM may take – violating the limits becomes not just technologically more difficult, but illegal as well.
- Criminal sanctions are available, under 17 U.S.C. § 506(a), for any willful infringement committed for commercial advantage or financial gain. Even where the motive

41 *MGM v. Grokster* 545 U.S. 913 (2005), *supra* note 28.

42 17 U.S.C. § 504(c)(1).

43 17 U.S.C. § 1201.

is not financial, willful infringement is criminal so long as the infringed works have a total retail value over $1,000.

- The 2008 PRO IP Act provides for civil forfeiture of any property used to commit or facilitate copyright violations.[44]

The continued existence of infringement should not be taken as evidence that these tools are too weak. Since eliminating infringement entirely is an impossible goal, it will *always* be possible to argue that legal remedies should be further expanded and that penalties and damages should be further ratcheted up. But this kind of never-ending one-way ratchet, resulting in copyright enforcement tools of ever-increasing reach and severity, would carry major costs for innovation and legitimate commerce. Policymakers aiming to improve copyright enforcement should look first to existing legal tools.

Importantly, however, the goal of making infringement less attractive compared to legal alternatives cannot be achieved by enforcement efforts alone. It also requires that copyright industries provide legal offerings that are compelling and convenient. Where government can promote the deployment of compelling legal offerings – for example, by streamlining existing statutes pertaining to music licensing – it should move aggressively to do so. And finally, as discussed in the next section, policymakers should look for opportunities to improve the public's understanding regarding the obligations of copyright law and the consequences of violating them.

2.6. Enforcement alone cannot solve online infringement. Increased availability of compelling legal options for obtaining copyrighted works and public education about the consequences of infringement are essential to reducing online infringement

A full strategy for reducing online infringement requires more than just the 'stick' of law enforcement. Just as essential is the 'carrot' of compelling legal offerings. One of the best defenses against infringement is the continued proliferation of lawful online distribution options that create convenient, easy-to-use ways for consumers to get the content they want in the form that they want it. When consumers have attractive legal options for satisfying their demand, the incentive to rely on illegal sources is greatly reduced. With this in mind, policymakers should look for ways to encourage the legal marketplace. For example, efforts to streamline licensing processes or reduce obstacles to using «orphan works» could open new avenues for the lawful distribution of copyrighted content, helping reduce infringement.[45]

---

44 Prioritizing Resources and Organization for Intellectual Property (PRO IP) Act of 2008. U.S. Pub. L. No. 110-403 (2008) § 303(a)(1).

45 CDT Policy Post (November 2, 2007). Music Rights Regime Needs Updating, Should Embrace New Technologies. Retrieved March 26, 2012, from http://cdt.org/policy/music-rights-regime-needs-updating-should-embrace-new-technologies; Curtis, Alex (2008). Orphan Works 2008: Senate and House Bills Introduced. *Public Knowledge blog*. Retrieved March 26, 2012, from http://www.publicknowledge.org/blog/orphan-works-2008-house-and-senate-bills-intr.

Public education is another important and underappreciated component of policy in this area. Modern information technology is here to stay and will continue to put powerful digital tools in the hands of the public. Inevitably, public attitudes and norms will play a major role in shaping how people choose to use the information-age tools at their disposal, including the extent to which they seek to engage in infringement. Public education is needed, therefore, to help shape consumer expectations and norms concerning the use of copyrighted works in a digital world. Copyright law can be a technical area, and consumers' initial assumptions about what is and is not permitted are often not fully accurate. Education about copyright infringement and its potential legal consequences also can help increase the deterrent effect that the legal framework and enforcement campaigns have on the general population.

In the absence of effective education to help the public better understand its rights and responsibilities in the copyright realm, evolving technological capabilities may create their own norms with little regard for law or policy. For reasons discussed in the previous sections, trying to contain infringement by restricting the development of new technological capabilities would carry heavy costs to innovation and free expression; such a strategy requires hobbling the very technologies that are central to the information economy. By contrast, trying to help shape the public's understanding of what are and are not appropriate *uses* of new technologies would pose no risk to innovation.

Influencing public norms around copyright may not be easy or quick. But if the goal is to have a long-term impact on the scope of the infringement problem without depressing expression-empowering innovation, policymakers should make public education a key part of the discussion.

3. CASE STUDY: TARGETING DOMAIN NAMES

In recent years, there has been considerable focus on using the domain name system (DNS) to go after websites associated with unlawful content. Since late June 2010, U.S. law enforcement agencies have executed seizure warrants for over 300 domains associated with copyright and trademark infringement as part of «Operation In Our Sites.»[46] The «PROTECT IP Act» and the «Stop Online Piracy Act,» introduced in the U.S. Senate and House of Representatives, respectively, would have given law enforcement the ability to compel ISPs and other DNS service providers to block domain-name lookup requests for certain non-U.S. websites in attempts to prevent potential users from reaching them.[47]

46 U.S. Immigration and Customs Enforcement (June 30, 2010). 'Operation In Our Sites' targets Internet movie pirates: ICE, Manhattan U.S. Attorney seize multiple Web sites for criminal copyright violations (Press Release). Retrieved March 26, 2012, from http://www.ice.gov/news/releases/1006/100630losangeles.htm.

47 Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (2011). S. 968. 112th U.S. Congress; Stop Online Piracy Act (2011). H.R. 3261. 112th U.S. Congress.

The DNS performs a relatively simple function: translating text URLs (like www.cdt.org) into machine-readable IP addresses (like 174.143.118.160). Seizing a domain name involves ordering the relevant registrar or registry to effectively revoke the website's domain-name registration, thus preventing the site from continuing to use that particular name. Blocking a domain name involves ordering a domain-name lookup service (for most users, a function performed by their ISP) not to respond to any user request to look up the IP address associated with that name.

Applying principles from the previous section reveals that the use of these tactics – while perhaps attractive to those seeking to block particular content – is unwise. They would be largely ineffective yet carry significant risk of collateral damage. Seizing and blocking domain names risk suppressing lawful expression and exacerbating cybersecurity risks, while doing little to stop infringement.

3.1. Principle 1: Focus on bad actors

Targeting domain names is a step removed from targeting actual infringing content, and is therefore quite likely to have an overbroad impact on innocent actors and legitimate expression. When domain-name tactics are used against websites with a mix of lawful and unlawful content, *all* the content is affected; there is no way to narrowly target the unlawful content only. This stands in sharp contrast to notice-and-takedown systems, which are typically used in the copyright context to address *specific* infringing material. Enforcement actions targeting a domain name itself would not be so narrowly targeted; they would affect anything and everything associated with that domain.

Moreover, a domain name frequently encompasses much more than just an individual website. Many web hosting services are constructed in a way such that thousands of individual sites, maintained by thousands of individuals, are hosted at subdomains sharing a single parent domain name. For example, the service might be located at «webhost.com» and the individual sites might be «joe.webhost.com» and «sara.webhost.com.» In addition, websites often share their domain names with non-web hosts, such as email and instant messaging servers. All of this speech stands to be affected if the domain name is seized or blocked.[48]

Indeed, a concrete example occurred in February 2011, when a U.S. law enforcement agency mistakenly seized the domain «mooo.com,» for hosting child sexual abuse images. Mooo.com turned out to be the parent domain of thousands of innocent and unrelated subdomains.[49] The owner of mooo.com allows individuals to register subdomains, which they can then point to any IP address. That means the mooo.com domain name is effectively subdivided and shared among numerous, entirely independent users. The content hosted at

48 In the U.S., such overblocking has led to at least one blocking law being ruled unconstitutional. *See CDT v. Pappert*. F. Supp. 2d 606 (ED Pa, 2004).

49 Claburn, Thomas (February 18, 2011). ICE Confirms Inadvertent Web Site Seizures. *Information Week*. Retrieved March 26, 2012, from http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=229218959&cid=RSSfeed_IWK_All.

any particular subdomain is wholly separate – hosted on different servers with different IP addresses – from the content hosted at other subdomains or at the first-level «mooo.com» domain itself. But because of illegal content allegedly present at one such subdomain, *all* were seized and redirected to a U.S. government banner announcing that the domain had been seized for violating child pornography laws.

The risk of affecting lawful content increases if seizure or blocking orders are issued without a full adversarial hearing, as has occurred under U.S. seizure law. A one-sided process, under which domain-name owners get no opportunity to defend themselves before their names are blocked or seized, creates significant potential for mistakes or overaggressive action. Again, several examples highlight this risk: sites seized in the U.S. include several music blogs who claim they had obtained the allegedly infringing material directly from rightsholders for promotional purposes,[50] as well as a Spanish site that has twice been found non-infringing by Spanish courts.[51]

In sum, seizing and blocking domain names can impede access to lawful material that simply shares a domain name with infringing material. This overbreadth makes the tactics unlikely to maintain a narrow focus on bad actors, and thus highly suspect from the perspective of online freedom of expression.

3.2. Principle 2: Avoid network-policing by intermediaries

While domain seizure and blocking policies would not necessarily impose liability for third-party actions on ISPs and domain registries, they clearly call on such intermediaries to serve as online enforcers against communications with targeted websites. As such, adoption of these policies would fundamentally alter the role of these critical intermediaries, transforming them from largely neutral service providers into content enforcers. Requiring ISPs in particular to attempt to block some communications of their subscribers would be a remarkable departure from well-established policy. The legislative safe harbors established in the U.S. and Europe represent a deliberate policy choice to allow ISPs to focus on empowering communications by and among users *without* monitoring, supervising, or playing any other gatekeeping role.

This policy choice is what has enabled the Internet's uniquely decentralized structure, which in turn has enabled the Internet to serve as an unprecedented platform for innovation, free expression, and economic growth. Given the lack of central supervision, it is also true that some people inevitably will use the network in connection with unlawful activity – just as some people use the road network or telephone network in connection with unlawful

50 Sisario, Ben (December 19, 2010). Music Web Sites Dispute Legality of Their Closing. *New York Times.* Retrieved March 26, 2012, from http://www.nytimes.com/2010/12/20/business/media/20music.html.

51 Anderson, Nate (February 2, 2011). US Customs begins pre-Super Bowl online mole-whack. *Ars Technica.* Retrieved March 26, 2012, from http://arstechnica.com/tech-policy/news/2011/02/us-customs-begins-pre-super-bowl-mole-whacking.ars.

activity. But decentralization is a core attribute of the Internet, and the policy choices that support it have been tremendously successful.

Importantly, there is no basis for thinking that the adoption of domain-focused tools for copyright enforcement would be just a minor exception to this important policy. Once the precedent has been established, there will be no principled basis for limiting the ISPs' policing role to copyright. There is no shortage of illegal or unsavory content on the Internet, and well-intentioned advocates for various causes would look to ISP domain-name blocking as the new tool for addressing it. As ISPs are enlisted for each new policy aim – however appropriate when viewed in isolation – the unsupervised, decentralized Internet would give way to a controlled, ISP-policed medium. This would be a fundamental change in how the Internet works.

3.3. Principle 3: Weigh costs versus benefits

A sober assessment of the likely costs and benefits of domain-focused enforcement reveals the folly of the approach.

In terms of benefits, domain seizure and blocking can each be easily circumvented, and thus will have little ultimate effect on levels of infringement. Neither seizing nor blocking a website's domain name removes the site – or any infringing content – from the Internet. The site and all its contents remain connected at the same IP address, and there are several ways a targeted site may still be reached.

In the case of a domain seizure, the site's operator could simply register a new domain name for the site. For example, most of the sports-streaming sites connected to ten domains seized in the U.S. in February 2011 quickly reappeared and are easily located at new domains. Alternatively or in addition, the site's operators could publicize its IP address, which users could then bookmark in lieu of saving or remembering the domain name. Or a site's operators could distribute a small browser plug-in or other piece of software to allow users to retrieve the IP addresses of the operators' servers. Such simple tools would make the process of following a site around the web virtually automatic.

The same tactics could be used to evade domain blocking. In addition, a site's users could easily switch DNS-lookup providers to avoid blocking orders. Savvy users could set up local DNS resolvers on their own computers, thus avoiding any DNS servers that have been ordered to block. Alternatively, third-party public DNS servers are widely available, and more would inevitably spring up to help evade blocking orders. For Internet users, pointing DNS requests to these unfiltered servers would be simply a matter of updating a single parameter in their operating systems' Internet settings. For users to whom this seems complicated, software tools could easily automate the process.[52]

All of these circumvention techniques are likely to occur if domain-name seizure and blocking become widespread. To the extent that sites hosting unlawful content have a highly

52 *See, e.g.,* DNS Jumper tool at http://sordum.3eeweb.com/?p=4573.

motivated and relatively savvy user base (as is often the case for sites and networks hosting copyright-infringing material), word would spread quickly as to how best to circumvent any blocking. This means that any impact from seizing or blocking domain names is likely to be ephemeral at best.

At the same time, the negative consequences of domain seizure and blocking appear substantial. As discussed above, these costs include the implications for free expression due to overbreadth. In addition, the particular tactic of blocking domain names presents a number of technical challenges that could have an impact on cybersecurity.[53]

First, for ISPs, compliance with blocking orders may come at the expense of implementing the DNS Security Extensions (DNSSEC). For over 15 years, Internet engineers have been working to develop and implement a set of standards for addressing security flaws in the domain name system.[54] But having DNS lookup providers either pretend a site does not exist or redirect users to a site they have not requested (such as to a site saying «access to the site you were seeking is being blocked due to illegal content») is flatly inconsistent with DNSSEC.[55] The incompatibility is technical; DNSSEC uses cryptography to prevent DNS responses from being tampered with or falsified. A DNS resolver using DNSSEC simply is not able to give a cryptographically signed response that is false. DNS lookup providers could try to avoid the incompatibility by declining to respond to certain DNS requests at all, but this can frustrate the development of secure applications that rely on DNSSEC, and carries performance and user-experience drawbacks that providers might prefer to avoid.[56]

Blocking at the DNS lookup-provider level carries security risks for Internet users beyond the tension with DNSSEC. Most users today rely on their ISPs to perform domain-name lookup functions. But as explained above with regard to ineffectiveness, switching to another lookup provider is trivial. The more ISPs and other major DNS providers are required to block lookup requests for websites that users want to reach, the more users will switch to independent, non-ISP DNS servers. And critically, they may not switch to other trustworthy DNS providers, but to DNS services located outside of the reach of blocking orders – likely to DNS servers operated by the very purveyors of the illegal content they wish to reach.

This would do more than just render service-provider-level domain-name blocking ineffective. ISPs' DNS servers offer a crucial window into network usage; migration away

53 A group of prominent DNS engineers has addressed these concerns in greater detail. S*ee* Steve Crocker et. al. (May 2011). *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill*. Retrieved March 26, 2012, from http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf.

54 *See, generally*, http://dnssec.net.

55 *See* Ofcom (U.K. telecom regulator) (August 3, 2011). 'Site Blocking' to reduce online copyright infringement. Retrieved March 26, 2012, from http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf. p. 43.

56 *See* Stewart Baker (December 14, 2012). SOPA Rope-a-dopa. *Skating on Stilts blog*. Retrieved April 30, 2012, from http://www.skatingonstilts.com/skating-on-stilts/2011/12/the-sopa-rope-a-dope.html.

from these servers would undermine ISPs' ability to observe and track botnet activity and other cybersecurity threats on their networks.

In addition, any such migration would put users at the mercy of potentially unscrupulous foreign DNS servers, which could redirect user traffic for phishing or botnet purposes. Though they may be unaware of it, users place an enormous amount of trust in their DNS provider to route requests to the proper sites. ISPs have incentive to maintain that trust, but other DNS operators – especially those with an interest in evading the blocking of sites dedicated to commercial infringement – will likely not share that same incentive. By creating strong incentives to rely on potentially untrustworthy DNS providers, the widespread use of domain-name blocking would create new and very dangerous opportunities for security risks and crime online.

These cybersecurity harms flow directly from the use of domain-name blocking to address objectionable content. In light of how ineffective the approach is likely to be, this should raise serious questions as to whether the approach is worth the risk.[57]

3.4. Principles 4 Through 6

The remaining principles are not as directly applicable to an evaluation of domain name–based tactics, but nonetheless offer some potentially useful considerations. Instead of mandatory DNS-blocking legislation of the type recently rejected by the U.S. Congress, it may be worth continuing to explore more voluntary and cooperative options. Similarly, efforts that emphasize education and improved lawful offerings may fare better from a cost-benefit standpoint. There is an argument that DNS-based enforcement can serve an educational role, but the potential educational impact is substantially undermined by the fact that DNSSEC makes it impossible for an ISP to redirect subscribers to an explanation or warning regarding infringement websites that are being blocked. Finally, setting a realistic goal counsels against the idea that policy must embrace virtually all available tactics, including domain seizure and blocking, in a vain attempt to close every loophole and leave no infringement scenario unaddressed.

4. CONCLUSION

The six principles laid out in this paper are intended to guide policymakers and law enforcement toward copyright enforcement tactics that do not compromise the openness and innovative potential of the Internet. Using these principles to evaluate tactics that focus on

57 Indeed, officials in the Obama administration wrote that copyright enforcement efforts must not compromise the security and integrity of the DNS. Espinel, Victoria, Aneesh Chopra, and Howard Schmidt (January 14, 2012). Combating Online Piracy while Protecting an Open and Innovative Internet. *Official White House Blog*. Retrieved March 26, 2012, from https://wwws.whitehouse.gov/petition-tool/response/combating-online-piracy-while-protecting-open-and-innovative-internet.

seizing and blocking access to domain names of infringing websites demonstrates that these measures fail to strike the appropriate balance. Ultimatley, focusing on domain names will do little to stop infringement, while altering the role of key intermediaries and doing harm to cybersecurity and free expression.

5. BIBLIOGRAPHY

Anderson, Nate (February 2, 2011). US Customs begins pre-Super Bowl online mole-whack. *Ars Technica.* Retrieved March 26, 2012, from http://arstechnica.com/tech-policy/news/2011/02/us-customs-begins-pre-super-bowl-mole-whacking.ars.

Baker, Stewart (December 14, 2012). SOPA Rope-a-dopa. *Skating on Stilts blog*. Retrieved April 30, 2012, from http://www.skatingonstilts.com/skating-on-stilts/2011/12/the-sopa-rope-a-dope.html.

Biddle, Peter et. al. (Microsoft 2002). *The Darknet and the Future of Content Distribution*. Retrieved March 26, 2012, from http://msl1.mit.edu/ESD10/docs/darknet5.pdf.

Booz & Co. The Impact of U.S. Internet Copyright Regulations on Early-Stage Investment (2011). Retrieved April 30, 2012, from http://www.booz.com/media/uploads/Booz-Co-Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf.

Burnham, Brad (March 13, 2012). «Freedom to Innovate» (Remarks at CDT Annual Dinner). Retrieved March 14, 2012, from http://www.usv.com/2012/03/the-freedom-to-innovate.php. (arguing that shortsighted regulations by the U.S. will push innovators and entrepreneurs to invest in countries outside the United States).

E-mail warnings deter Canadians from illegal file sharing. *CBC News* (February 15, 2007). Retrieved March 25, 2012, from http://www.cbc.ca/consumer/story/2007/02/14/software-warnings.html.

Center for Democracy & Technology (CDT) (2010). *Protecting Copyright and Internet Values: A Balanced Path Forward*. Retrieved March 26, 2012 from http://www.cdt.org/copyright/20050607framing.pdf.

CDT (November 2, 2007). Music Rights Regime Needs Updating, Should Embrace New Technologies. Retrieved March 26, 2012, from http://cdt.org/policy/music-rights-regime-needs-updating-should-embrace-new-technologies.

CDT (March 2, 2010). Statement before the Senate Judiciary Committee, Subcommittee on Human Rights and the Law: *Global Internet Freedom and the Rule of Law II*. 111th Congress, 2nd Sess. Available at http://www.cdt.org/files/pdfs/20100302_cdt_global_net_freedom.pdf.

Claburn, Thomas (February 18, 2011). ICE Confirms Inadvertent Web Site Seizures. *Information Week*. Retrieved March 26, 2012, from http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=229218959&cid=RSSfeed_IWK_All.

Secretary of State Hillary Rodham Clinton (January 21, 2010). Remarks on Internet Freedom, address at The Newseum. Retrieved from http://state.gov/secretary/rm/2010/01/135519.htm.

Computer and Communications Industry Association (CCIA) (2011). *Fair Use in the U.S. Economy: Economic Contributions of Industries Relying on Fair Use*. Retrieved March 25, 2012 from http://www.ccianet.org/CCIA/files/ccLibraryFiles/Filename/000000000526/CCIA-FairUseintheUSEconomy-2011.pdf.

Crocker, Steve, et. al. (May 2011). *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill*. Retrieved March 26, 2012, from http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf.

Curtis, Alex (2008). Orphan Works 2008: Senate and House Bills Introduced. *Public Knowledge blog*. Retrieved March 26, 2012, from http://www.publicknowledge.org/blog/orphan-works-2008-house-and-senate-bills-intr.

Espinel, Victoria, Aneesh Chopra, and Howard Schmidt (January 14, 2012). Combating Online Piracy while Protecting an Open and Innovative Internet. *Official White House Blog*. Retrieved March 26, 2012, from https://wwws.whitehouse.gov/petition-tool/response/combating-online-piracy-while-protecting-open-and-innovative-internet.

Memorandum of Understanding between U.S. copyright industries and ISPs (July 6, 2011). Retrieved March 26, 2012, from http://www.copyrightinformation.org/sites/default/files/Momorandum%20of%20Understanding.pdf.

French Constitutional Council (June 10, 2009). Decision regarding the Law Promoting the Diffusion and Protection of Creativity on the Internet, Law No. 2009-669. Retrieved March 25, 2012, from http://www.conseil-constitutionnel.fr/decision.42666.html.

Kafka, Peter (February 11, 2010). «Veoh finally calls it quits: Layoffs yesterday, bankruptcy filing soon.» *CNet*. Retrieved March 26, 2012 from http://news.cnet.com/8301-1023_3-10452152-93.html.

U.S. Government Accountability Office (April 2010). *Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*. Retrieved March 26, 2012, from www.gao.gov/new.items/d10423.pdf.

U.S. Immigration and Customs Enforcement (June 30, 2010). 'Operation In Our Sites' targets Internet movie pirates: ICE, Manhattan U.S. Attorney seize multiple Web sites for criminal copyright violations (Press Release). Retrieved March 26, 2012, from http://www.ice.gov/news/releases/1006/100630losangeles.htm.

Sisario, Ben (December 19, 2010). Music Web Sites Dispute Legality of Their Closing. *New York Times.* Retrieved March 26, 2012, from http://www.nytimes.com/2010/12/20/business/media/20music.html.

Sohn, David (July 2011). ISPs and Copyright Owners Strike a Deal. *CDT Policy Beta blog*. Retrieved March 23, 2012, from https://www.cdt.org/blogs/david-sohn/isps-and-copyright-owners-strike-deal.

Stelter, Brian (August 15, 2008). Some Media Companies Choose to Profit From Pirated YouTube Clips. *New York Times*. Retrieved March 25, 2012, from http://www.nytimes.com/2008/08/16/technology/16tube.html?_r=1.

Tehranian, John (2007). Infringement Nation: Copyright Reform and the Law/Norm Gap. In Utah Law Review 537. http://ssrn.com/abstract=1029151.

World Intellectual Property Organization (WIPO) (2011), *Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries (Preliminary Version)*. Retrieved March 23, 2012, from http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries.pdf.

Laws, Bills, and Directives

U.S. Copyright Act. 17 U.S.C. § 101 *et. seq.*

«Section 230» of U.S. Communications Act. 47 U.S.C. § 230.

U.S. Digital Millennium Copyright Act (DMCA). 17 U.S.C. §§ 512, 1201.

Family Home Movie Act of 2005. U.S. Pub. L. no. 109-9 (2005) § 110(11).

Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (2011). S. 968. 112th U.S. Congress.

Stop Online Piracy Act (2011). H.R. 3261. 112th U.S. Congress.

Prioritizing Resources and Organization for Intellectual Property (PRO IP) Act of 2008. U.S. Pub. L. No. 110-403 (2008) § 303(a)(1).

European Union Directive 2000/31/EC on electronic commerce. Available at http://ec.europa.eu/internal_market/e-commerce/directive_en.htm.

Cases

Sony Corp. of America v. Universal City Studios, Inc. 464 U.S. 417 (1984).

RIAA v. Diamond Multimedia Systems, Inc. 180 F.3d 1072 (9th Cir. 1999).

Kelly v. Arriba Soft Corporation. 336 F.3d 811 (9th Cir. 2003).

CDT v. Pappert. F. Supp. 2d 606 (E.D. Pa, 2004).

Chamberlain Group, Inc. v. Skylink Technologies, Inc. 381 F.3d 1178 (Fed. Cir. 2004).

Lexmark International, Inc. v. Static Control Components, Inc. 387 F.3d 522 (6th Cir. 2004).

MGM Studios, Inc. v. Grokster, Ltd. 545 U.S. 913 (2005).

Storage Tek v. Custom Hardware. 421 F.3d 1307 (Fed. Cir. 2005).

The Authors Guild, et. al., v. Google, Inc. 05 CV-8136 (DC) (S.D.N.Y 2005).

UMG Recordings, Inc. v. Grouper, Inc. CV 06-06561 (C.D. Ca. 2006).

UMG Recordings, Inc., et al. v. Bolt, Inc., et. al. CV 06-06577 (C.D. Cal. 2006).

Clean Flicks of Colo., LLC v. Soderbergh. 433 F. Supp. 2d 1236 (D. Colo. 2006).

Perfect 10, Inc. v. Amazon.com, Inc. 508 F.3d 1146 (9th Cir. 2007).

Capitol Records, LLC., et. al. v. VideoEgg. 08 CV-5831 (S.D.N.Y. 2008).

UMG Recordings, Inc. v. MySpace, Inc. CV 06-7361 AHM (AJWx) (C.D. Cal. 2008).

The Cartoon Network LP, et al., v. CSC Holdings, Inc. and Cablevision Sys. Corp. 536 F.3d 121 (2nd Cir. 2008), *cert. denied* 129 S. Ct. 2890.

UMG Recordings, Inc. v. Shelter Capital Partners LLC 2011 WL 6357788 (9th Cir. Dec. 20, 2011).

U.S. v. ASCAP (In re Application of Cellco Partnership d/b/a/ Verizon Wireless). 663 F. Supp. 2d 363 (S.D.N.Y 2009).

Tiffany Inc. v. eBay, Inc. 600 F.3d 93 (2nd Cir. 2010).

Viacom Int'l, Inc., v. YouTube, Inc. 10-3270-cv, 2012 WL 1130851 (2nd Cir. April 5, 2012).

Io Group, Inc. v. Veoh Networks, Inc. 586 F. Supp. 2d 1132.

PIPA, SOPA, OPEN – THE END OF PIRACY OR PRIVACY?

László Németh[1]
PhD Student[2], Institute of Comparative Law,
Faculty of Law, University of Szeged

ABSTRACT: After the Combating Online Infringement and Counterfeits Act (COICA) could not pass the 111th Congress of the United States of America, Vermont Democrat Senator Patrick Leahy proposed another bill to the 112th Congress in May 2011, entitled Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA). This time the House of Representatives were not able to accept this proposal, so they made their own version in October 2011 with the name Stop Online Piracy Act (SOPA). It had an even stricter ruling than its «older brothers» and was the focus of world-wide criticism.

From the beginning there was one member of the Senate, who raised his voice against these bills: Oregon Democrat Ron Wyden. With the help of California Republican Representative Darrell Issa they made their own proposal in December 2011, Online Protection and Enforcement of Digital Trade Act (OPEN Act).

What is common in these bills? They are against 'non-domestic Internet sites', that is all the sites not located in the United States. If they found something infringing the US copyrights, they would be able to shut these sites down. It does not matter, if the material is originally offered from Hungary, Egypt or Russia.

How would it be possible? How do they want to regulate the whole Internet and how does it affect online privacy? Would this be the solution against piracy?

I will try to answer these questions from a European point of view, also examining the possibility of a similar regulation in the European Union. Should we do the same to the United States, what they are planning against us?.

KEYWORDS: COICA, PIPA, SOPA, OPEN, ACTA, net neutrality, copyright law.

1. INTRODUCTION

Nowadays the Internet has a major role in our life. Modern people use it to access the news from the world, to keep in touch with others, to have fun by watching movies and listening to songs online. Its importance is growing every day. It is not a surprise, that the governments know this as well. They want to check and control the time spent online, even by

1 The author wishes to thank Samantha Cheesman for language revision and Péter Mezei for the useful comments.

2 The Project named „TÁMOP-4.2.1/B-09/1/KONV-2010-0005 – Creating the Center of Excellence at the University of Szeged» is supported by the European Union and co-financed by the European Regional Development Fund.

blocking specific sites and services. Not to mention the mammoth companies that offer tons of services – they simply follow us on the Internet and can show us the advertisements we are really interested in. It is harder to protect the online privacy than the one in the real world.

The main reason of this «surveillance» is definitely money. The entertainment industry never liked the ones, who use their contents without paying for it. That is obvious, no one would like it. They think this world-spread phenomenon, usually mentioned as piracy, is the real source of evil. Anyone who illegally downloads a movie or a song should get his punishment. Even if they have to do this by breaking into his privacy by retrieving data from his ISP. Not surprisingly, the United States of America is leading these campaigns. They made several bills and proposals concerning the topic. The first part of this paper is dealing with these texts and their effects. Afterwards I will provide an outlook of the European Union and examine the possibility of similar legislation within this region. I think there may be a good solution to this problem, but we should check every possible aspect in order to have a strong opinion about this question.

2. ACTS, BILLS AND PROPOSALS IN THE UNITED STATES

2.1. The Basics

In order to get the answer, why it is very important to the United States to rule the Internet, we can approach the question from three directions.

2.1.1. Network Architecture

The Internet is a worldwide network that was built systematically. Not surprisingly, it was originally designed for military purposes in the United States, but later it became available for the public.[3] Andrés Guadamuz divides networks into physical and logical levels in his recent article. The more interesting is the «logical architecture, where the USA has managed to remain considerably ahead of other countries. While anyone can create an Internet server by just installing the appropriate software onto any computer connected to the Web, you need a registrar if you want a domain name that resolves in the system (such as technollama.co.uk). Most top level domains are registered in the USA (.com, .org, .net, .biz), and statistics show that the US is the country with the most domain names registered under its jurisdiction, with 78,453,258 in late January 2012. The closest country is Germany with over six million registrations. In fact, not even combining all of the other countries in the world can you reach the total of domains registered in the USA.»[4]

---

3 Leiner, B. M., et al (n.d.) *Brief History of the Internet. Internet Society.* Retrieved March, 20th, 2012 from http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet

4 Guadamuz, A. (2012). *SOPA and Network Architecture. Society for Computers & Law.* Retrieved March, 7th, 2012 from http://www.scl.org/site.aspx?i=ed24747 However, it is hard to believe that China has not even got at least 6 million domain names to claim the second place.

This is the physical and logical reason, why the United States feel that they have to protect the network that was basically created by them. They think the Internet is *their* network, so they are allowed every means to protect it from the others, who want to use it to cause harm to the US.

2.1.2. Network Neutrality

When speaking about networks, we should mention network neutrality as well. The expression was created by Tim Wu in 2003.[5] Its essence is the fact, that on the Internet everyone has to be equal. There should be no way to differentiate between users, who may get the same information sooner than someone else (or even who may get some information, which someone else could not get at all).[6] One of the first documents about this topic was the U.S. Federal Communications Commission's (FCC) *Broadband Policy Statement* in 2005. In this paper they laid down four important principles. «To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet:

1) consumers are entitled to access the lawful Internet content of their choice.
2) consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement
3) consumers are entitled to connect their choice of legal devices that do not harm the network
4) consumers are entitled to competition among network providers, application and service providers, and content providers.»[7]

In 2010, FCC again stated the same in the *Open Internet Order*.[8]

Law professors also think it was necessary to speak about network neutrality. Lawrence Lessig and Robert McChesney stated: «Without net neutrality, the Internet would start to look like cable TV. A handful of massive companies would control access and distribution of content, deciding what you get to see and how much it costs. Major industries such as health care, finance, retailing and gambling would face huge tariffs for fast, secure Internet use –all

5 Wu, T. (2003). Network Neutrality, Broadband Discrimination. *Journal of Telecommunications and High Technology Law, Vol. 2.,* p. 141. Retrieved March, 7th, 2012 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863

6 On the topic I would recommend the following books: Cerrillo-i-Martinez, A., Peguera, M., Peña-López, I., & Vilasau Solana, M. (2011). *Net Neutrality and other challenges for the future of the Internet*. Barcelona: Huygens Editorial and Marsden, C. T. (2010). *Net Neutrality – Towards a Co-Regulatory Solution.* New York: Bloomsbury Academic.

7 U.S. Federal Communications Commission (2005). *Policy Statement.* Retrieved March, 19th, 2012 from http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf

8 U.S. Federal Communications Commission (2010). *FCC Acts To Preserve Internet Freedom and Openness.* Retrieved March, 19th, 2012 from http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-303745A1.pdf

subject to discriminatory and exclusive dealmaking with telephone and cable giants.»[9] Even the president of the United States, Barack Obama deemed the question very important and provided support to the Net Neutrality Plan of FCC.[10]

2.1.3. Legislation

Clay Shirky states in a video presentation[11] that the media industry drives the whole legislation process[12]. Companies founded in the 20th century do not tolerate the needs of modern people – what is not just consuming, but creating, publishing and sharing. He thinks the first step in the process was the *Audio Home Recording Act* (AHRA) of 1992.[13] In this act the Congress differentiated between legal and illegal copying of copyrighted materials. Shirky says that the industry was not satisfied with the outcome. So in the *Digital Millennium Copyright Act* (DMCA)[14] they introduced the protection of DRM technology[15] (practically the circumvention of DRM protection on copyrighted materials is deemed to be a copyright infringement).

At the end of the 20th century a bigger threat to the media industry began to spread. This was the world of Internet, where you can find everything (whether for money or for free) if you look for it. People started to use file-sharing services and these services were soon ended in front of a court.[16] The community pages such as Facebook, YouTube, Twitter, etc. got so many users, that one simply cannot follow their activity. People are sharing everything nowadays. As Shirky said: «Some of the stuff we share is stuff we've made. Some of the stuff we share is stuff we've found. Some of the stuff we share is stuff we've made out of what we've found, and all of it horrifies those industries.»[17] Most of these things are protected by

---

9 Lessig, L., McChesney, R. (2006). *No Tolls On The Internet. Washington Post.* Retrieved May, 27th, 2011 from http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060702108.html

10 Albanesius, C. (2009). *Obama Supports Net Neutrality Plan. PC Mag.* Retrieved May, 27th, 2011 from http://www.pcmag.com/article2/0,2817,2353195,00.asp

11 Shirky, C. (2012). *Why SOPA is a bad idea?* Retrieved March, 21st, 2012 from http://www.ted.com/talks/lang/en/defend_our_freedom_to_share_or_why_sopa_is_a_bad_idea.html

12 See Litman, J. (2006). *Digital Copyright*. New York: Prometheus Books.

13 *Audio Home Recording Act of 1992* (1992). Retrieved March, 20th, 2012 from http://thomas.loc.gov/cgi-bin/query/z?c102:S.1623.ENR:

14 *Digital Millennium Copyright* Act (1998). Retrieved March, 20th, 2012 from http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281.ENR:

15 To sum it up, DRM is the reason why one cannot copy his lawfully bought DVD disc only for making a backup of it, because there is a built-in feature that blocks this option. If someone cracks it, he will have to take the consequences of infringing copyright.

16 Just think of the Napster case, for example. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (2001).

17 Shirky, C. (2012).

copyrights, even if the users cannot recognize this. The media industry thinks they have to be punished somehow for these violations. However, there is no time and money to bring everyone in front of the court. This is why Shirky is of the opinion, that the media companies convinced the ones in the legislation system to make laws to create fear in the people. Fear of doing anything «wrong».

So the *Combating Online Infringement and Counterfeits Act* (COICA)[18] was reported in the Senate on 18th November 2010 by Vermont Democrat Senator Patrick Leahy[19]and the avalanche started to roll. It was against «Internet sites dedicated to infringing activities» and provided an *in rem* action to the Attorney General against the domain name itself, even if the registry or registrar of it was not located in the United States. It is very important, that in this bill the court had to determine «whether an Internet site conducts business directed to residents of the United States».[20] The bill passed the Senate Judiciary Committee, but never received a full vote on the Senate floor. The main problem was that the 111th U.S. Congress ended on 3rd January 2011, so simply there was too little time to pass this bill.

2.2. PIPA

The *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act* (PROTECT IP Act, PIPA) was introduced[21] to the Senate (during the 112th U.S. Congress) on 12th May 2011. Its sponsor was the aforementioned Patrick Leahy. After a two week debate, it was reported[22] to the Senate on 26th May 2011. It is a successor of COICA, but it has so many new things, that we have to deal with it in detail. Let us take a look at them.

Section 3 is dealing with «rogue websites operated and registered overseas». This means a procedure against an «Internet site dedicated to infringing activities»[23] located outside the United States. Basically we are speaking about domain names (eg www.google.com). The most important fact is that the United States want to give themselves an extraterritorial jurisdiction with this step,[24] which is very problematic not just in the case of copyright law, but

18 *Combating Online Infringements and Counterfeits Act* (2010). Retrieved March, 21st, 2012 from http://thomas.loc.gov/cgi-bin/query/z?c111:S.3804:

19 *Patrick Leahy – United States Senator for Vermont.* Retrieved March, 21st, 2012 from http://www.leahy.senate.gov/

20 COICA Section 2 (c) (2) (B).

21 *To Prevent Online Threats To Economic Creativity And Theft Of Intellectual Property, And For Other Purposes.* (2011). Retrieved December, 8th, 2011 from http://www.leahy.senate.gov/imo/media/doc/BillText-PROTECTIPAct.pdf

22 *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act* (2011). Retrieved March, 20th, 2012 from http://thomas.loc.gov/cgi-bin/query/z?c112:S.968:

23 PIPA Section 2 (7).

24 Against domestic sites they already have the *Operation In Our Sites* programme run by the U.S. Immigration and Customs Enforcement (ICE). See: *«Operation In Our Sites» targets Internet movie pirates.*

mostly in case of private international law. Section 4 is about 'eliminating the financial incentive to steal intellectual property online', taking care of both domestic and nondomestic websites. What is common in these sections is the two-step procedure. At first, there may be an *in personam* action[25] against the registrant of the domain name or the owner or operator of an Internet site dedicated to infringing activities.[26] The difference between the sections is in the person who may commence the action: in case of rogue websites it is the Attorney General, in case of Section 4 the so-called «qualifying plaintiffs».[27] If they cannot find the one responsible for the domain name, the second step comes alive, which is an *in rem* action. They simply block this domain in order for it not to be available to the public.[28] However, what really makes me wonder is the provision, that one can «modify, suspend or vacate the order [...] any time *after* the issuance of an order».[29] In this way one cannot complain before they shut down his domain name, just after they have done it. Instead of the presumption of innocence we have *presumption of guilt* now. One can only defend himself after proven guilty, even if he is not.

After the main dish the dessert comes in Section 5, what is «voluntary action against websites stealing American intellectual property». Some kind of service providers (eg. domain name registrars, financial transaction providers, etc.) can voluntarily shut down the suspicious domain names instead of the authority. If they do so, they will enjoy immunity from liability. It has benefits only for these providers, not for the users or the domain names.

After heavy protests (see below) the bill was finally withdrawn by unanimous consent in Senate on 23rd January 2012.

2.3. SOPA

After seeing the mistakes in PIPA, Texas Republican Lamar Smith[30], a member of the House of Representatives introduced another bill. It has the short title *Stop Online Piracy Act*

(2010) Retrieved May, 27th, 2011 from http://www.ice.gov/news/releases/1006/100630losangeles.htm

25 That is the biggest innovation of the bill: they want to find persons now, not just web sites.

26 PIPA Section 3 (a) (1) and Section 4 (a) (1).

27 PIPA Section 2 (11).

28 This was a real concern for those who can understand the structure of Internet. Domain names were created just to be easily remembered. The computers communicate with each other in the language of numbers. Every Internet site has its own number code, called IP-address. For example the above mentioned www.google.com's IP address is 74.125.227.102 (as of 20th March 2012). Just try it: copy-paste these numbers to your web browser, and if it has not been changed since the closure of the manuscript, you will find yourself on www.google.com. So taking away the domain names will not affect the Internet as they wanted.

29 PIPA Section 3 (f) (1) and Section 4 (f) (1), emphasis added.

30 *Congressman Lamar Smith – 21st District of Texas.* Retrieved March, 21st, 2012 from http://lamarsmith.house.gov/

(SOPA).[31] It is divided into two bigger parts. Title I has almost the same structure as PIPA. In Section 101, amongst the definitions, a huge mistake of PIPA is corrected. The bill is talking about not just domain names, but IP addresses as well. Now this raises real concerns, because blocking them as well would block the whole Internet.

Sections 102 and 103 are similar to Sections 3 and 4 of PIPA. The «Internet site dedicated to infringing activities» has changed to «foreign infringing site» and «Internet site dedicated to theft of U.S. property» in the text. Again, the Attorney General and the qualifying plaintiffs may commence the *in personam*, then the *in rem* actions. However, there is a very important amendment. The whole text is about the infringing «Internet site or portion thereof». This means if there was a tiny little thing that allegedly infringed the copyright of anyone from the United States; the whole site could be shut down. Imagine this: someone shares something infringing on Netlog.[32] According to this bill, the whole of Netlog should be blacked out. Its domain name and IP address should be blocked. In my opinion this does not make any sense. Naturally, as we could see in PIPA, one can modify, suspend or vacate the order against his site only *after* receiving the order. However, for the sites that are taking «voluntary action against sites dedicated to theft of U.S. property»[33] and «against sites that endanger public health»[34] immunity is granted.

Title II has more interesting provisions as well. Section 201 is dealing with the «streaming of copyrighted works in violation of criminal law». Section 203 is about «protecting U.S. businesses from foreign and economic espionage». Section 205 is the punch line of the whole text. It is «defending intellectual property rights abroad». They want to appoint an intellectual property attaché in every major geographic region in order to protect the copyrights of U.S. citizens. I think this is not the best solution. Every nation should protect the rights of copyright holders efficiently, so the United States would not have to overstep their borders.

After the growing discontent of the people worldwide, more and more senators and representatives opposed SOPA (and PIPA as well). On 20th January 2012 the House voting of SOPA was indefinitely postponed.[35]

2.4. PIPA and SOPA – concerns, objections, protests

There were so many ways of expressing the main concerns against these bills. New York Times' Rebecca MacKinnon named SOPA «The Great Firewall of America» in one of her

31 *Stop Online Piracy Act* (2011). Retrieved March, 20th, 2012 from http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.3261:

32 http://www.netlog.com

33 SOPA Title I Section 104.

34 SOPA Title I Section 105. However, it is really interesting to read such things in a bill that was originally meant to defend copyrights.

35 You can see the whole timeline of PIPA/SOPA legislation at *Timeline of SOPA and PIPA Actions and Statements*. Retrieved March, 20th, 2012 from http://projects.propublica.org/sopa/timeline

articles.[36] She was not the only one who was afraid of the possible effects of SOPA on free speech: other bloggers[37] raised their voice on this topic as well.

Some companies decided upon the written way of protesting. «On November 15, Google, Facebook, Twitter, Zynga, eBay, Mozilla, Yahoo, AOL, and LinkedIn wrote a letter[38] to key members of the U.S. Senate and House of Representatives, saying SOPA poses 'a serious risk to our industry's continued track record of innovation and job creation, as well as to our nation's cybersecurity.'»[39] Another letter[40] was written by law professors, who raised their concerns, too. «Laurence Tribe, a high-profile Harvard law professor and author of a treatise titled American Constitutional Law, has argued[41] that SOPA is unconstitutional because, if enacted, 'an entire Web site containing tens of thousands of pages could be targeted if only a single page were accused of infringement.'»[42] Leonard Napolitano, Sandia National Laboratories' director of computer sciences and information systems «warned in a letter that the legislation is 'unlikely to be effective' and will 'negatively impact U.S. and global cybersecurity and Internet functionality.'»[43] Signatures were also collected opposing the bills.[44]

However, the biggest online event was the January 18 Blackout Day. Thousands of Internet sites expressed their protests against the bills. «Wikipedia's English-language pages went completely black at 9 p.m. PT, with a splash page saying 'the U.S. Congress is considering legislation that could fatally damage the free and open Internet.' [...]Google's home

36 MacKinnon, R. (2011). *Stop the Great Firewall of America. New York Times.* Retrieved March, 19th, 2012 from http://www.nytimes.com/2011/11/16/opinion/firewall-law-could-infringe-on-free-speech.html

37 Gattuso, J., Rosenzweig, P. (2012). *Free Speach: An Unintended Victim of Protect IP and SOPA? The Heritage Foundation.* Retrieved March, 19th, 2012 from http://blog.heritage.org/2012/01/18/free-speech-an-unintended-victim-of-protect-ip-and-sopa/

38 *SOPA – Google, Facebook, Twitter Letter* (2011). Retrieved March, 19th, 2012 from http://politechbot.com/docs/sopa.google.facebook.twitter.letter.111511.pdf

39 McCullagh, D. (2012a). *How SOPA would affect you: FAQ. CNET News.* Retrieved March, 7th, 2012 from http://news.cnet.com/8301-31921_3-57329001-281/how-sopa-would-affect-you-faq/

40 *An Open Letter To The House Of Representatives* (2011). Retrieved March, 19th, 2012 from http://politechbot.com/docs/sopa.law.professor.letter.111511.pdf

41 Tribe, L. H. (2011). *The «Stop Online Piracy Act» (SOPA) Violates The First Amendment.* Retrieved March, 19th, 2012 from http://www.scribd.com/doc/75153093/Tribe-Legis-Memo-on-SOPA-12-6-11-1

42 McCullagh, D. (2012a).

43 McCullagh, D. (2011a). *Sandia Labs: SOPA will 'negatively impact' U.S. cybersecurity. CNET News.* Retrieved March, 7th, 2012 from http://news.cnet.com/8301-31921_3-57326956-281/sandia-labs-sopa-will-negatively-impact-u.s-cybersecurity/

44 The most interesting thing about this campaign that it was jointly made by a liberal and a conservative group. Obviously there are situations, when one should put aside his political opinions. Gross, G. (2012a). *Groups Launch Campaign Against Lawmakers Supporting SOPA, PIPA. PC World.* Retrieved March, 7th, 2012 from http://www.pcworld.com/businesscenter/article/248337/groups_launch_campaign_against_lawmakers_supporting_sopa_pipa.html

page featured a big, black block over the colorful 'Google' logo that dominates the page, and a stark message under the search window urged: 'Tell Congress: Please don't censor the web!'»[45] Also, there were street protests in several American cities, where thousands of people went outside to raise their voice (and banners) against the legislation and to preserve the Internet in its current state.[46] However, some people think the work is not done, until these bills irrevocably disappear.[47]

Naturally, there were many supporters of these bills. The number of the cosponsors in the Senate of PIPA[48] and in the House of Representatives of SOPA[49] was however constantly diminishing as time advanced.[50] Those who did not want to lose their voters rather backed out of supporting the proposals. Three big organizations, the Motion Picture Association of America (MPAA), the Recording Industry Association of America (RIAA)[51] and the U.S. Chamber of Commerce[52] were all defending PIPA/SOPA. As one can expect, Hollywood was also a «huge fan» of these bills.[53] However, when even the White House[54] stated that they

45 McCullagh, D. (2012b). *Wikipedia, Google blackout sites to protest SOPA. CNET News.* Retrieved March, 7th, 2012 from http://news.cnet.com/8301-31921_3-57360754-281/wikipedia-google-blackout-sites-to-protest-sopa/

46 Paul, I. (2012). *Were SOPA/PIPA Protests a Success? The Results Are In. PC World.* Retrieved March, 7th, 2012 from http://www.pcworld.com/article/248401/were_sopapipa_protests_a_success_the_results_are_in.html

47 Gross, G. (2012b). *SOPA, PIPA Opponents Celebrate, but Say Work Isn't Done. PC World.* Retrieved March, 7th, 2012 from http://www.pcworld.com/article/248423/sopa_pipa_opponents_celebrate_but_say_work_isnt_done.html

48 *Cosponsors of PIPA.* Retrieved March, 20th, 2012 from http://thomas.loc.gov/cgi-bin/bdquery/z?d112:SN00968:@@@P

49 *Cosponsors of SOPA.* Retrieved March, 20th, 2012 from http://thomas.loc.gov/cgi-bin/bdquery/z?d112:HR03261:@@@P

50 Especially after the White House made its statement (see below). Block, A.B. (2012a). *Support Diminishing for Anti-Piracy Bills SOPA, PIPA. The Hollywood Reporter.* Retrived March, 20th, 2012 from http://www.hollywoodreporter.com/news/sopa-pipa-anti-piracy-bills-protests-283047 See also the PIPA/SOPA timeline in footnote 35.

51 *Analysis: Rogue Sites Bill Enjoys Rare, Extensive Bipartisan Support. (n.d.) RIAA – Recording Industry Association of America.* Retrieved March, 20th, 2012 from http://riaa.com/newsitem.php?content_selector=newsandviews&news_month_filter=11&news_year_filter=2011&id=B74C7B2B-68EC-EBE9-6CB9-946F517749B1

52 McCullagh, D. (2011b). *SOPA's most aggressive defender: U.S. Chamber of Commerce. CNET News.* Retrieved March, 20th, 2012 from http://news.cnet.com/8301-31921_3-57334409-281/sopas-most-aggressive-defender-u.s-chamber-of-commerce/

53 Block, A.B. (2012b). *Hollywood Guilds Release Statement of Support for SOPA on Day of 'Blackout' Protests- The Hollywood Reporter.* Retrieved March 20th, 2012 from http://www.hollywoodreporter.com/news/sopa-blackout-protests-dga-sag-statement-support-283028

54 Remember the opinion of President Barack Obama on net neutrality – he kept his word about that topic.

would not support neither SOPA or PIPA,[55] the media industry got really angry. «'We just feel very let down by the administration and Obama for not supporting us,' one studio chief reportedly said. [...] 'At least let him remain neutral and not go against it until we can get the legislation right,' one mogul reportedly said. 'But Obama went against it. I'm personally not going to support him anymore and not give a dime anymore.' [...] 'God knows how much money we've given to Obama and the Democrats and yet they're not supporting our interests,' one studio head told Deadline.»[56] These were the reactions of the frustrated media industry after the story practically ended. Just for the record, Representative Lamar Smith had another bill previously, with the name *Protecting Children From Internet Pornographers Act of 2011*.[57] «Jim Hood, the Democratic attorney general of Mississippi, and co-chair of a National Association of Attorneys General committee on the topic, recently likened[58] rogue Web sites to child porn.»[59] I think there is a possibility, that they will link the two things together in a brand new bill in the foreseeable future.

2.5. OPEN Act

Oregon Democrat Senator Ron Wyden[60] opposed these bills right from the beginning. He already intended to object to COICA, and then became «the most committed and longest opponent of SOPA and PIPA»[61] by placing hold on PIPA on 26th May 2011.[62] He even threatened to filibuster the bill in November. «'The at-all-cost approaches that these bills take to protecting intellectual property sacrifices cybersecurity while restricting free speech and innovation,' [Wyden] added. 'Congress needs to hear from more than the lobbyists who helped write these bills. Congress needs to hear from people like you, who understand the

55 Smith, C. (2012). *White House Will Not Support SOPA, PIPA. The Huffington Post.* Retrieved March, 20th, 2012 from http://copyrightinthexxicentury.blogspot.com/2012/01/breaking-news-sopa-rip.html

56 Newman, J. (2012). *Hollywood Disappointed With President Obam's SOPA Stance. PC World.* Retrieved March, 20th, 2012 from http://www.pcworld.com/article/248425/hollywood_disappointed_with_president_obamas_sopa_stance.html

57 *Protecting Children From Internet Pornographers Act of 2011 (2011).* Retrieved March, 21st, 2012 from http://thomas.loc.gov/cgi-bin/bdquery/z?d112:hr1981:

58 Hood, J. (2011). *Congress needs to pass rogue sites bill to protect the Internet. The Hill's Congress Blog.* Retrieved March, 22nd, 2012 from http://thehill.com/blogs/congress-blog/technology/192605-congress-needs-to-pass-rogue-sites-bill-to-protect-the-internet

59 McCullagh, D. (2012a)

60 *Senator Ron Wyden.* Retrieved March, 22nd, 2012 from http://wyden.senate.gov/

61 Franzen, C. (2012). *The OPEN Act Introduced; Can It Kill SOPA and PIPA? Taling Points Memo Idea Lab.* Retrieved March, 22nd, 2012 from http://idealab.talkingpointsmemo.com/2012/01/the-open-act-introduced-can-it-kill-sopa-and-pipa.php

62 *Press Release of Senator Wyden – Wyden Places Hold on Protect IP Act* (2011). Retrieved March, 22nd, 2012 from http://wyden.senate.gov/newsroom/press/release/?id=33a39533-1b25-437b-ad1d-9039b44cde92

value of a fair and free Internet.'»[63] However, the cloture motion[64], that ended PIPA's short life, was filed by Nevada Democrat Senator Harry Reid.[65]

Wyden really meant what he said. On 8th December 2011 he launched a website with the help of California Republican Representative Darrell Issa.[66] It is the site «Keep The Web Open».[67] They posted a draft of a new possible bill, which became the *Online Protection and Enforcement of Digital Trade Act* (OPEN Act). It was introduced in the Senate by Wyden on 17th December 2011 and a slightly modified version in the House of Representatives by Issa on 18th January 2012. Basically it is an amendment to the Tariff Act of 1930.[68] The biggest innovation of this proposal was that anyone could add his comments and suggestions to the bill with the help of the website of the two Congressmen. «The OPEN Act, alongside SOPA and PIPA, seek[s] to essentially write a Bill of Rights for the Web. In that spirit, the editing tool used on the OPEN Act's Web site is named after James Madison, the author of the original Bill of Rights. The Web site for the OPEN Act displays a quote from Madison as a pretense for the public interaction with the bill: 'Knowledge will forever govern ignorance; and people who mean to be their own governors must arm themselves with the power which knowledge gives.'»[69] This is «a new way of thinking about the legislative process – a Wiki-ed out, crowdsourced, digitized version of bill writing.»[70]

If we read through the text of the bill, we can see some similarities with PIPA and SOPA, but the differences are more important. First of all, it is again about «Internet site[s] dedicated to infringing activity,» but the definition is really narrower, because it means a site «(i) is accessed through a nondomestic domain name; (ii) conducts business directed to residents of the United States; and (iii) has only limited purpose or use other than engaging

63 Gross, G. (2011). *Senator Threatens Filibuster of Protect IP Act as Vote Nears. PC World.* Retrieved March, 22nd, 2012 from http://www.pcworld.com/businesscenter/article/244622/senator_threatens_filibuster_of_protect_ip_act_as_vote_nears.html

64 *Cloture Filed on the Motion to Proceed to S.968, PROTECT IP* (2011). Retrieved March, 22nd, 2012 from http://democrats.senate.gov/2011/12/17/cloture-filed-on-the-motion-to-proceed-to-s-968-protect-ip/

65 *Senator Harry Reid*. Retrieved March, 22nd, 2012 from http://www.reid.senate.gov/

66 *Congressman Issa.* Retrieved March, 22nd, 2012 from http://issa.house.gov/

67 *KeepTheWebOpen.com.* Retrieved March, 22nd, 2012 from http://keepthewebopen.com/

68 *19 USC Chapter 4 – Tariff Act of 1930.* Retrieved March, 22nd, 2012 from http://uscode.house.gov/download/pls/19C4.txt

69 Walton, Z. (2012). *The OPEN Act Becomes Truly Open – Citizens are invited to rewrite bill with the help of Madison. WebProNews.* Retrieved March, 22nd, 2012 from http://www.webpronews.com/open-act-truly-open-2012-01

70 Sutter, J.D. (2012). *The OPEN Act as an experiment in digital democracy. CNN.* Retrieved March, 22nd, 2012 from http://whatsnext.blogs.cnn.com/2012/01/18/the-open-act-as-an-experiment-in-digital-democracy/

in infringing activity and whose owner or operator primarily uses the site [for infringing copyrights].»[71] There are also exclusions from this definition, too.

Another innovation is that instead of the Attorney General, the U.S. International Trade Commission should investigate in case of violations. Not just close a web site without saying anything, the Commission *may* investigate on its own initiative and *shall* investigate upon receiving a complaint from «the owner of a copyright or trademark that is the subject of the infringing activity alleged in the complaint.»[72] No words on blocking sites, the Domain Name System (DNS), search engines, anything. However, there is a really interesting thing: «If the Commission determines under paragraph (1) that an Internet site dedicated to infringing activity is operated or maintained in violation of subsection (b), the Commission shall promptly submit to *the President* a copy of the determination, the record upon which the determination is based, and any order issued under subsection (f) pursuant to the determination.»[73] I do not understand why we should involve the President in such a case.

The rest of the bill contains similar provisions that were also included in PIPA and SOPA. The «Modification or Revocation of Orders»[74] now really makes sense, because orders can be issued after all the previously mentioned conditions are met and the site contains infringing material. Immunity is a sure thing as well, that could not be left out.

So, once again, what are the main differences from the previous bills? «OPEN would give oversight to the International Trade Commission (ITC) instead of the Justice Department, focuses on foreign-based websites, includes an appeals process, and would apply only to websites that 'willfully' promote copyright violation. SOPA and PIPA, in contrast, would enable content owners to take down an entire website, even if just one page on it carried infringing content, and imposed sanctions after accusations –not requiring a conviction.»[75] As Representative Issa told the press: «'OPEN is a targeted, effective solution to the problem of foreign, rogue websites stealing from American artists and innovators […] Today's Internet blackout has underscored the flawed approach taken by SOPA and PIPA to the real problem of intellectual property infringement. OPEN is a smarter way to protect taxpayers' rights while protecting the Internet.'»[76]

Naturally, the once-sponsors of PIPA and SOPA did not like the new proposal. Lamar Smith stated: «The OPEN Act creates loopholes that make the Internet even more open to foreign thieves that steal America's technology and IP without protecting U.S. businesses

71 OPEN Act, Section 2 (a) (8).

72 OPEN Act, Section 2 (d) (1).

73 OPEN Act, Section 2 (e) (4) (A), emphasis added.

74 OPEN Act, Section 2 (f) (3).

75 DesMarais, C. (2012). *SOPA, PIPA Stalled: Meet the OPN Act. PC World.* Retrieved March, 22nd, 2012 from http://www.pcworld.com/article/248525/sopa_pipa_stalled_meet_the_open_act.html

76 Gross, G. (2012c). *Issa introduces SOPA alternative in the House. Computer World.* Retrieved March, 22nd, 2012 from http://www.computerworld.com/s/article/9223541/Issa_introduces_SOPA_alternative_in_the_House

and consumers. It amounts to a safe harbor for foreign criminals who steal American technology, products and intellectual property.»[77] Also, «[t]he MPAA has publicly spoken out against the OPEN act saying that it is 'ineffective in targeting foreign criminal websites', and is 'time-consuming and costly for copyright holders to [act] against foreign thieves'. They are also concerned with the speed and effectiveness of the ITC, a government organization that usually deals with minor internal patent laws. [...] Finally, the MPAA believes that this draft 'goes easy on internet piracy,' and does not go far enough to effectively prevent it.»[78] Not surprisingly, the RIAA criticized it, too. «'The OPEN Act does nothing' to stop online infringement and 'may even make the problem worse,' the industry group says in a statement it is circulating on Capitol Hill this week. 'It does not establish a workable framework, standards, or remedies. It is not supported by those it purports to protect.'»[79]

At the time of closing this manuscript, neither of the previous bills has been enacted. OPEN Act is getting really close to it (it has more cosponsors than the others had in the Congress), but Wyden, Issa and the others have to fight the lobby of the media industry. This will not be simple. However, maybe the result will please both sides, if they can talk about it in a democratic way.

3. THE EFFECTS OF SOPA AND PIPA IN THE EUROPEAN UNION

As you read above, PIPA and SOPA are dealing with foreign infringing internet sites and domain names. So this is not an internal, rather an international problem. What are the main European concerns with these bills? If we want to make fun of it, just listen to the Swedish Home Affairs Commissioner Cecilia Markström, who noted, «that 'sopa' in Swedish means garbage.»[80] However, to keep a straight face, we must focus on the real problems. «The main arguments against SOPA and PROTECT IP are that they would lead to internet censorship, hamper free speech (including non-infringing speech) and result in an increased monitoring of internet activities, thus invading user privacy. Moreover, it is feared that the bills would negatively impact legitimate websites hosting user-created content, disrupt the internet-based economy and harm the basic structure and architecture of the internet. [...] Because the bills are not directed at US-based websites only, but at any website that is ac-

77 *OPEN Act Increase Bureaucracy, Won't Stop IP Theft* (2012). Retrieved March, 22nd, 2012 from http://judiciary.house.gov/news/01192012.html

78 sammieman (2012). *The OPEN act: An Overview of the SOPA Alternative. IGN.* Retrieved March, 22nd, 2012 from http://www.ign.com/blogs/sammieman/2012/01/22/the-open-act-an-overview-of-the-sopa-alternative

79 Lee, T.B. (2012) *Shoe on the other foot: RIAA wants to scrap anti-piracy OPEN Act. Ars technica.* Retrieved March, 22nd, 2012 from http://arstechnica.com/tech-policy/news/2012/02/shoe-on-the-other-foot-riaa-calls-for-open-act-to-be-scrapped.ars

80 Anonymous (2012). *Europe's SOPA? Gulf Stream Blues.* Retrieved March, 23rd, 2012 from http://gulfstreamblues.blogspot.com/2012/01/europes-sopa.html

cessible in the US, it is feared that they affect a large number of websites worldwide. This is especially so because the legal definitions in SOPA and PROTECT IP are so broad and imprecise that these bills target not only pirate websites, but also jeopardize websites and online business models with a legitimate aim.»[81]

Showing the importance of the situation, even some Members of the European Parliament (led by Marietje Schaake from The Netherlands) sent a letter to the US Congress expressing their concerns. «We, Members of the European Parliament, civil society organizations and businesses would like to draw your attention to the extra territorial effects of current intellectual property rights (IPR) enforcement acts being proposed in the US Congress. The two houses are expected to vote on the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PROTECT IP) and the Stop Online Piracy Act (SOPA). […]

We are concerned that SOPA and PROTECT IP will be detrimental to internet freedom, internet as a driver for economic growth and for fundamental rights, not only in the EU, but globally. The legitimate aim is to halt infringements of intellectual property rights online. However, since the internet is used for nearly every aspect of citizens' lives, business activity or government regulation, the effects of these acts will lead to enormous collateral damage.

The acts suggest blocking of websites by court order or in the Domain Name System (DNS), a worldwide resource and essential component for the functionality of the internet. Not only the infringing part of a website would be blocked, but a whole domain would be made inaccessible, thereby violating the freedom of expression. Further, by blocking at the DNS level, these websites would be made inaccessible far beyond US jurisdiction, as the websites would be inaccessible worldwide.»[82]

They also questioned the vague definitions and the liability issues. They also referred to European law cases in connection with the monitoring and filtering problems: «The European Court of Justice has recently ruled in the Scarlet/SABAM case that monitoring and filtering of communication online is a breach of fundamental rights such as privacy, freedom of communication and freedom of information and should not be applied to halt infringements of IPR.»[83]

Another Dutch politician, Neelie Kroes, Vice President of the European Commission chose the modern way of expressing her opinion about the topic. She wrote messages on Twitter. She was «'glad [the] tide is turning on #SOPA; don't need bad legislation when should be safeguarding benefits of open net,' and claimed that '[s]peeding is illegal too: but you don't put speedbumps on the motorway.'»[84] Kroes also said that «'there is no #EU

81 Van Gompel, S. (2012). *European concerns with SOPA. Kluwer Copyright Blog.* Retrieved March, 23rd, 2012 from http://kluwercopyrightblog.com/2012/01/18/european-concerns-with-sopa/

82 *Letter to US Congress* (2011). Retrieved March, 23rd, 2012 from http://euletter-sopa-pipa.tumblr.com/post/14113460718/final-letter-with-signatures

83 *Letter to US Congress* (2011).

84 Ingraham, N. (2012). *Neelie Kroes, VP of the European Commission, speaks out against SOPA. The Verge.* Retrieved March, 23rd, 2012 from http://www.theverge.com/2012/1/20/2720648/neelie-kroes-sopa-objection-tweet-vp-european-commission

version of #SOPA. Internet reg must be effective, proportionate, preserve benefits of open net.'»[85] Viviane Reding, the European Commissioner for Justice, Fundamental Rights and Citizenship similarly stressed, that «'You'll never have from Europe a blocking of the Internet –that's not the European option.' [...] If she meant it, then that's an extremely important line [being drawn] in the sand given that the blocking of sites has already started in Finland, the Netherlands, and the UK.[86] It will be interesting to see if she and her colleagues back those words up with any action.»[87] This just leads us back to the problem of net neutrality. The world walked away with PIPA and SOPA, «[b]ut there is an international agreement which some internet freedom advocates say is just as bad as SOPA, and it is heading toward a speedy passage in the EU. It is called ACTA, or the Anti-Counterfeiting Trade Agreement.»[88] The effects of ACTA cannot be seen right now.

4. CONCLUSIONS

When the Internet began to spread and the web started to really go world wide, the World Intellectual Property Organization (WIPO) made the so-called Internet Treaties in 1996. The *WIPO Copyright Treaty* (WCT)[89] and the *WIPO Performances and Phonograms Treaty* (WPPT)[90] were basically updates of the previous international agreements, but they had to «address the challenges posed by the digital technologies advancements, in particular the dissemination of protected material over digital networks such as the Internet.»[91] However, the Internet has changed and they were simply not able to follow this.

I think nowadays we do not need just American, European, etc. agreements, acts, laws. We need another international treaty like the WTC and WPPT that should regulate the

85 Neal, D. (2012). *European Commission VP Neelie Kroes opposes SOPA. The Inquirer.* Retrieved March, 23rd, 2012 from http://www.theinquirer.net/inquirer/news/2140257/european-commission-vp-neelie-kroes-opposes-sopa

86 See: Davies, CJ. (2009). *The Hidden Censors Of The Internet. Wired Magazine.* Retrieved May, 27th, 2011 from http://www.wired.co.uk/magazine/archive/2009/06/features/the-hidden-censors-of-the-internet

87 Moody, G. (2012). *Blocking The Net 'Not The European Option' –EU Comissioner Reding. TechDirt.* Retrieved March, 23rd, 2012 from http://www.techdirt.com/articles/20120123/05544117513/blocking-net-not-european-option-eu-commissioner-reding.shtml

88 Anonymous (2012). ACTA was signed by the European Commission and 22 European Union member states on 26th January 2012.

89 *WIPO Copyright Treaty* (1996). Retrieved March, 23rd, 2012 from http://www.wipo.int/export/sites/www/treaties/en/ip/wct/pdf/trtdocs_wo033.pdf

90 *WIPO Performances and Phonograms Treaty* (1996). Retrieved March, 23rd, 2012 from http://www.wipo.int/export/sites/www/treaties/en/ip/wppt/pdf/trtdocs_wo034.pdf

91 *WIPO Internet Treaties.* Retrieved March, 23rd, 2012 from http://www.wipo.int/copyright/en/activities/wct_wppt/wct_wppt.html

situation. Most importantly: we have to ask the people who are using the Internet in the end. Just like Congressmen Wyden and Issa did. We need this new form of democracy. Instead of «Internet Treaties», we need «Web 2.0» or «User-generated Treaties.» The Internet has changed so as have the users. We can find something copyright-infringing on barely every website (either just a picture, or even a video). In my opinion the biggest fault of the aforementioned American bills was the idea, that in every case the whole site should be blocked, not just the infringing content. However, examining every little sub-site requires time and resources. Who would be able to do this job? I can see two possible options for this:

1) an automatic system that is checking and filtering the websites,[92] or
2) individuals who are doing this.

However, even I can argue that this would be successful. Both options require lots of money. In case 1), there is the real risk of mistakes being made – no automatic system nowadays can think like a human. In case 2), the salaries would be really high, so I think filtering is not really the most effective way to prevent infringing activities. I would say prevention is more important than punishment. If the users have more opportunities and cheaper goods, they would not turn to piracy. Because of this I personally do not like the American bills: that would give the United States international control over the Internet. For example, in a research that I am currently participating in we checked the prices of the same DVD's in Hungary and in the United States.[93] The average price of a Hungarian DVD is around $ 13, compared to the American $ 17. However, there are bigger differences in the wages between the two countries. In Hungary the annual average wage was $ 12,843 in 2010. In the United States this number is $ 40,560.[94] This discrepancy between the wages of the two countries is really interesting. Having less money does not guarantee you the right to infringe copyrights. However, it should not be the base for the richer country to judge you and completely block the site you are running.

As I have mentioned before: we need an international ruling, not national laws with international effects. The content-producers should see that they have to decrease their need for money and offer alternative sources for the users. However, the other side should also implement changes as well. This is why it is important and a good idea to include the users in the legislation process. If they feel themselves important (eg. by getting more rights and not examined closely by filtering their Internet traffic), probably they would not infringe the copyrights. We should find an agreement between these two sides. I do not know, if ACTA could be a good starting point for this, but on the aforementioned «Keep The Web Open»

92 However, monitoring is prohibited both in the United States (DMCA Chapter 5, §512 (m)) and in the European Union (Directive 2000/31/EC of the European Parliament and of the Council, Chapter 2 Article 15). The service providers cannot seek illegal activity continuously. They should handle every case individually.

93 *DVD árak*. Retrieved April, 25th, 2012 from http://dl.dropbox.com/u/18150734/dvdarak.xls

94 *List of countries by average wage.* Retrieved April, 25th, 2012 from http://en.wikipedia.org/wiki/List_of_countries_by_average_wage

site now one can comment and express his feelings about this agreement. In the fight against piracy we cannot win without leaving people their privacy. Not everyone using the Internet for sharing things is a pirate. We should keep that in mind.

5. BIBLIOGRAPHY

5.1. Books, Articles

Cerrillo-i-Martinez, A., Peguera, M., Peña-López, I., & Vilasau Solana, M. (2011). *Net Neutrality and other challenges for the future of the Internet*. Barcelona: Huygens Editorial.

Litman, J. (2006). *Digital Copyright*. New York: Prometheus Books.

Marsden, C. T. (2010). *Net Neutrality – Towards a Co-Regulatory Solution.* New York: Bloomsbury Academic.

Wu, T. (2003). Network Neutrality, Broadband Discrimination. *Journal of Telecommunications and High Technology Law, Vol. 2.,* p. 141.

5.2. Legal Bases

Audio Home Recording Act of 1992

Combating Online Infringements and Counterfeits Act (2010)

Digital Millennium Copyright Act (1998)

Online Protection and Enforcement of Digital Trade Act (2012)

Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (2011)

Protecting Children From Internet Pornographers Act of 2011

COMUNICACIONES SOBRE COMERCIO ELECTRÓNICO Y JUEGO ONLINE

¿CÓMO INFLUIRÁ LA NUEVA DIRECTIVA 2011/83/UE EN EL COMERCIO ELECTRÓNICO?

Zofia Bednarz
Estudiante de posgrado de la Universidad de Málaga

RESUMEN: Esta comunicación se centra en analizar el impacto que tendrá la nueva Directiva 2011/83/UE, sobre los derechos de los consumidores, en el ámbito del comercio electrónico tanto a nivel nacional como europeo. Actualmente, esta Directiva constituye no sólo el principal instrumento de protección de los consumidores en el ámbito del comercio electrónico, sino también trata de eliminar los obstáculos que impiden el correcto funcionamiento del mercado interior. Sin embargo, la Propuesta inicial de la Directiva no tuvo una acogida favorable ni por parte de los académicos ni por los comerciantes que actúan en el ámbito electrónico. Aunque la Directiva ha sido objeto de diversas modificaciones a lo largo de su proceso de adopción, algunas reglas controvertidas acaban de entrar en vigor. En esta comunicación se trata de analizar las novedades introducidas por la Directiva en materia del comercio electrónico, como por ejemplo la regla de la armonización plena que abarca a la información precontractual y el derecho de desistimiento. La Directiva establece también las normas relativas a la compra y descarga del contenido digital. Las nuevas normas, sobre todo aquellas que sobrecargan a los comerciantes con nuevos deberes y obligaciones, causarán el incremento del riesgo financiero de las empresas presentes en el ámbito electrónico. En consecuencia, los precios de bienes y servicios vendidos en línea subirán y los consumidores deberán pagar su propia protección. Además, demasiada regulación introducida por la Directiva probablemente producirá la ralentización del mercado, que constituye un efecto indeseable en la época de la crisis.

PALABRAS CLAVE: Directiva 2011/83/UE, comercio electrónico, consumidores, contratación a distancia, comerciantes.

1. INTRODUCCIÓN

Sólo una parte de las normas establecidas por la nueva Directiva 2011/83/UE sobre los derechos de los consumidores está destinada a regular el comercio electrónico con los consumidores. Se puede señalar otra directiva correspondiente al comercio electrónico, la Directiva 2000/31/CE. No obstante, esta Directiva abarca sobre todo las cuestiones «técnicas» relacionadas con contratación a través de Internet. La nueva Directiva 2011/83/UE está enfocada hacia las relaciones contractuales y la protección de los consumidores que adquieren bienes y servicios en línea. No sólo los consumidores, sino también los comerciantes esperaban la adopción de esta Directiva desde hace mucho tiempo. La Directiva 2011/83/UE ha sido objeto de numerosos debates y discusiones sobre todo en lo que respecta al comercio electrónico. Todos los afectados –las instituciones de la Unión Europea, las asociaciones de consumidores y de comerciantes, los Estados Miembros– intentaban a hacer prevalecer sus propios intereses. En esta ponencia se trata de analizar si las esperanzas puestas en la Directiva se alcanzarán y cuál será su influencia en el comercio electrónico.

La Directiva 2011/83/UE es una de las directivas relativas al derecho de contratos. Las normas que regulan la contratación, especialmente la contratación con consumidores, están cada vez más influidas por la normativa europea. En el derecho europeo de contratos la autonomía de la voluntad de las partes constituye un principio de igual importancia que la necesidad de proteger a la parte más débil económicamente y menos informada[1]. La contratación electrónica se puede definir como una de las modalidades de contratar, sin embargo es una modalidad de contratar especial. Por un lado, a la contratación electrónica se le aplican las mismas reglas, que a la contratación en general, por otro existe normativa dedicada únicamente a la contratación electrónica. Analizando la Directiva relativa a los derechos de consumidores y su influencia en el comercio electrónico no se puede olvidar la existencia de la extensa normativa destinada, entre otros, a la contratación con consumidores y a las condiciones generales de contratación que también tiene una gran trascendencia para el comercio electrónico. Sin embargo, esta ponencia se centra principalmente en el análisis de la nueva Directiva 2011/83/UE y su significado para el comercio electrónico con participación de los consumidores.

2. PROPUESTA DE LA DIRECTIVA RELATIVA A LOS DERECHOS DE LOS CONSUMIDORES

2.1. Obstáculos al comercio electrónico transfronterizo

La Directiva 2011/83/UE (DO L 304 de 25.10.2011, p.64) sobre los derechos de los consumidores fue propuesta por la Comisión Europea con el objeto de eliminar los obstáculos que impiden el correcto funcionamiento del mercado interior europeo. El comercio electrónico constituye un elemento de gran importancia para el funcionamiento del mercado interior al ser una de las vías que permite mantener relaciones contractuales entre comerciantes y consumidores independientemente de las fronteras. Sin embargo, conforme a lo dispuesto en el Considerando (5) de la propia Directiva, no se está aprovechando plenamente el potencial de las ventas transfronterizas a distancia. El crecimiento de esta modalidad de transacciones nacionales durante los últimos años ha sido mucho más importante que el de las transacciones internacionales a nivel europeo, como lo señala la Comisión en su Comunicación[2]. La Comisión añade también que la Unión Europea todavía está muy lejos de llegar a explotar todo el potencial económico del comercio electrónico. En los países G8, Corea del Sur y Suecia, «la economía de Internet» *(internet*

1 Grundmann, S. (2011). The Future of Contract Law. *European Review of Contract Law, 4/2011,* 490-527. p.500

2 Así también la Comisión Europea: *¨Although the growth rate of e-commerce at national level is high, this new vector remains marginal at only 3.4% of European retail*¨ en:
Commission Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: *A coherent framework for building trust in the Digital Single Market for e-commerce and online services* COM(2011) 942 p.1

economy) ha generado un 21% del crecimiento del PIB en los últimos cinco años, mientras que la participación de «la economía de Internet» en el PIB europeo es muy limitada. En comparación con otras regiones del mundo, como Estados Unidos o Asia–Pacífico el comercio electrónico europeo está menos avanzado y se limita principalmente al nivel nacional.

Para proponer la Directiva, la Comisión se apoyó en el Libro verde sobre la revisión del acervo en materia de consumo[3], en el cual está demostrado que en la Unión Europea no sólo los consumidores, sino también los empresarios desconfían de la venta transfronteriza a través de Internet. Para los empresarios, según los estudios Eurobarómetro, citados en el Libro verde, la fragmentación jurídica en el mercado interior, debida a la regla de la armonización mínima, utilizada en la mayoría de las directivas relativas a la protección del consumidor, constituye un factor disuasorio importante. Se cree que es una de las principales causas de la ralentización del comercio transfronterizo, ya que supone un considerable incremento de gasto para las empresas. Como demuestran las encuestas mencionadas, los consumidores tampoco aprovechan la posibilidad de obtener bienes y servicios a través de Internet en otros Estados Miembros. La razón de esta situación según el Libro verde también parece ser la incertidumbre jurídica. La Directiva en el Considerando (6) también se basa en la conclusión de que ciertas disparidades jurídicas entre Estados Miembros crean obstáculos significativos en el funcionamiento del mercado interior.

Sin embargo, existen otros factores que también pueden influir en la confianza de los contratantes y en el crecimiento de ventas transfronterizas a través de Internet. Los consumidores eligen bienes y servicios y deciden principalmente en función del precio y por lo tanto, el interés de un consumidor en perfeccionar un contrato en línea depende igualmente de los costes de entrega de la cosa comprada. Como era de esperar, normalmente estos costes varían según destino, pero sorprendentemente el precio no depende estrictamente de la distancia, sino del país de destino[4]. La entrega nacional es generalmente la más barata, es decir la entrega de una tienda *on-line* situada en Barcelona a Málaga cuesta menos que la entrega a Perpignan, cuando desde Barcelona hasta Málaga hay 1000 km y desde Barcelona hasta Perpignan: 200 km[5]. También el idioma empleado por el comerciante tiene trascendencia para la posibilidad de llevar a cabo un negocio en línea transfronterizo. El comerciante que tiene la intención de vender en otros Estados Miembros debe llevar a cabo la traducción de su página web y de la publicidad. El coste de esta traducción es comparable al coste de la asesoría jurídica que necesitaría el comerciante para ajustarse a la normativa de la protección de consumidores en otro Estado Miembro. Estos factores no han sido tomados en considera-

3 Libro verde sobre la revisión del acervo en materia del consumo COM(2006) 744 final

4 Los ejemplos de tarifas de las empresas de envios:
SEUR: http://pages.ebay.es/sellercentral/seur/precios_y_servicios.html
MAIL BOXES: http://wwww.mbe.es/index.php?id=34
DHL: http://www.dhl.com.pl/content/dam/downloads/pl/express/brochures/dhl_int_price_list_july_2011_en.pdf

5 Un ejemplo de la tienda *on-line* que sigue estas reglas: http://www.stand-up-surf.com/shop/index.php

ción por la Comisión en el proceso de adopción de la Directiva a pesar de que pueden influir en la confianza de los consumidores y comerciantes del mismo modo que la fragmentación jurídica de normas[6].

2.2. El significado de las consultas públicas

Después de la adopción del Libro verde, la Comisión llevó a cabo consultas públicas para responder a la pregunta ¿cómo se habría podido simplificar y completar el marco normativo vigente?[7] Cabe destacar que esta encuesta fue tenida en cuenta por la Comisión en el proceso de adopción de la Directiva[8], llegando la Comisión a la conclusión que la fragmentación jurídica de normas es un obstáculo principal para el comercio transfronterizo. En las consultas participaron todos los Estados Miembros, salvo Dinamarca, las instituciones públicas nacionales y europeas, las organizaciones de consumidores, los comerciantes y empresarios, los académicos y otros, en total más de 300 sujetos. No obstante, contrariamente a lo que sostiene el Informe citado, parece que el numero de encuestados no es tan significativo ya que en la Unión Europea hay 493 millones de consumidores[9] y 20 millones de empresarios[10]. A pesar de que obviamente no todos estos profesionales mantienen relaciones comerciales con consumidores, se puede observar que 300 encuestados es un número muy bajo y ello a pesar de que empresas de gran importancia como Apple o Deutsche Bank han participado en las consultas. La mayoría de encuestados han indicado que la armonización plena de ciertos aspectos de transacciones nacionales y transfronterizas puede constituir una solución a los problemas relacionados con los obstáculos al comercio *business to consumer*. En la Propuesta la Comisión pone de manifiesto, que la armonización plena de ciertos aspectos de los contratos con consumidores tendría como efecto el aumento de la seguridad jurídica para ambas partes, consumidores y comerciantes. No obstante, no aporta ninguna prueba, salvo la encuesta mencionada[11].

---

6 Twigg – Flesner, Ch., Metcalfet, D. (2009) The proposed Consumer Rights Directive – less haste, more thought? *European Review of Contract Law, 3/2009*, 368-391. p.372

7 Commission Staff Working Paper: *Report on the Outcome of the Public Consultations on the Green Paper on the Review of the Consumer Aquis* http://ec.europa.eu/consumers/cons_int/safe_shop/acquis/acquis_working_doc.pdf

8 Propuesta de Directiva del Parlamento Europeo y del Consejo sobre derechos de los consumidores, COM(2008)614 final. p.4

9 Estrategia comunitaria en materia de política de los consumidores 2007-2013, Luxemburgo 2007 http://ec.europa.eu/consumers/overview/cons_policy/doc/cps_0713_es.pdf p.5

10 Schieman, M. (2008). Enterprises by size class – overview of SMEs in the EU. *Eurostat. Statistics in focus,* 31/2008 http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-08-031/EN/KS-SF-08-031-EN.PDF

11 Micklitz, H.-W., Reich, N. (2009) Crónica de una muerte anunciada: The Commission Proposal for a Directive on Consumer Rights, *Common Market Law Review, 46/2009,* 471–519. p. 477

2.3. La acogida de la Propuesta de la Directiva

Aunque la iniciativa de llevar a cabo una nueva directiva relativa a los derechos de consumidores tuvo muy buena acogida por considerarse necesaria[12], las opiniones sobre la Propuesta de la Directiva han sido generalmente negativas. En primer lugar, una cuestión ampliamente criticada[13] fue la regla general de la armonización plena con muy pocas excepciones establecida en la Propuesta. Surgían dudas sobre si la armonización plena sería o no fuente de un aumento de la confianza en las relaciones transfronterizas de consumidores y empresarios[14]. Además, se ha puesto de manifiesto que la consecuencia de la introducción de la regla de armonización plena significaría para los consumidores en algunos Estados Miembros la disminución del nivel de protección[15].

Aparte del nivel de la armonización, la Propuesta igualmente provocó criticas en otras áreas. Por un lado se señaló que carecía de relación con proyectos académicos del derecho europeo de contratos, tales como PECL y DCFR[16], proyectos cuya elaboración había apoyado la Comisión. Asimismo la terminología utilizada en la Propuesta tuvo mala acogida, se indicó sobre todo su imprecisión[17]. A todo ello cabe añadir la indeterminación e inexactitud de normas establecidas en la Propuesta, por ejemplo la falta de remedios por incumplimiento, cuestión que llamó la atención de los académicos y juristas europeos[18].

También los comerciantes que actúan en el ámbito electrónico criticaron el proyecto de la Directiva durante su proceso de adopción[19]. Las asociaciones de comerciantes de varios Estados Miembros se preocuparon sobre todo por el derecho de desistimiento otorgado a los

---

12 Aubert de Vincelles, C. (2011). Perspectives for European Consumer Law. Towards a Directive on Consumer Rights and Beyond, H. Schulte-Nölke and L. Tichy (eds), Sellier, 2010: Book Review. *European Review of Contract Law, 4/2011,* 567-572. p. 568

13 Howells, G., Reich, E. N. (2010) Extent of Harmonisation in Consumer Contract Law. Note on the level of harmonization. *European Parliament. Directorate General for Internal Policies. Policy Department C: Citizens' Rights and Constitutional Affairs. Legal Affairs.* PE 432.728 http://www.europarl.europa.eu/studies p. 6 y la literatura allí citada

14 Así por ejemplo: Deshayes, O. (2011) Réponse du LEJEP au Livre vert de la Commission européenne. http://ec.europa.eu/justice/news/consulting_public/0052/contributions/91_fr.pdf, p.6; Micklitz, H.-W., Reich, N. (2009) Crónica de una muerte...*cit*. p. 474

15 Twigg – Flesner, Ch., Metcalfet, D. (2009) The proposed Consumer Rights Directive...*cit.* pp. 372-373

16 Así: Micklitz, H.-W., Reich, N. (2009) Crónica de una muerte...*cit.* pp. 473, 493,
Twigg – Flesner, Ch., Metcalfet, D. (2009) The proposed Consumer Rights Directive...*cit.* p. 369,
Hesselink, M. W. (2009). The Consumer Rights Directive and the CFR: two worlds apart?, *European Review of Contract Law, 3/2009,* 290-303

17 Aubert de Vincelles, C. (2011). Perspectives for European Consumer Law...*cit.* p. 568

18 *Idem*

19 UEAMPE open letter http://www.ueapme.com/IMG/pdf/Letter_to_perm_reps_May_2011.pdf
European industry associations open letter http://www.e-commercefacts.com/news/2011/05/branch-organisations-cons/index.xml

consumidores en los contratos a distancia y la obligación de comerciantes de soportar todos los costes relacionados con la devolución del producto comprado por consumidor.

Durante el proceso legislativo el proyecto de la Directiva fue debatido en el Consejo y el Parlamento Europeo siendo objeto de varias modificaciones por lo que la Directiva adoptada dista mucho de la Propuesta inicial. El Parlamento Europeo ha tenido en cuenta la mayoría de las opiniones criticas expresadas con respecto a la Propuesta, y resultado de ello fue el cambio de las reglas más controvertidas acerca de la armonización plena[20]. Sin embargo, algunas reglas controvertidas, como por ejemplo las relativas a los costes de devolución del bien, han sido mantenidas en la Directiva y acaban de entrar en vigor.

3. DIRECTIVA ADOPTADA

3.1. Texto definitivo de la Directiva 2011/83/UE

La versión final de la Directiva 2011/83/UE fue adoptada el 25 de octubre 2011, la cual deroga las Directivas: 97/7/EC, relativa a la protección de los consumidores en materia de contratos a distancia y 85/577/EEC, relativa a la protección de los consumidores en el caso de contratos negociados fuera de los establecimientos comerciales. Además la Directiva modifica las Directivas 93/13/EEC, sobre las cláusulas abusivas en los contratos celebrados con consumidores y 1999/44/EC, sobre determinados aspectos de la venta y las garantías de los bienes de consumo. La nueva Directiva regula la contratación a distancia y fuera de los establecimientos mercantiles y también algunos aspectos de todas las modalidades de contratos perfeccionados con consumidores, es decir, sobre todo el deber de los comerciantes de facilitar a los consumidores un determinado conjunto de información precontractual. Del ámbito de aplicación de la Directiva queda excluida una serie de contratos, conforme a su art. 3, por ejemplo contratos relativos a los servicios sociales, los bienes inmuebles, los juegos por dinero o los servicios financieros.

La Directiva tiene el objetivo de establecer un conjunto de reglas claras y uniformes en toda la Unión Europea para asegurar por un lado mejor protección de los consumidores y por otro un funcionamiento del mercado interior sin obstáculos. Como la revisión del acervo en materia de consumo ha demostrado la fragmentación jurídica de las normas, debida principalmente a la armonización mínima y también a la incoherente regulación de algunas cuestiones en distintas directivas[21], la nueva Directiva pretende establecer reglas más uniformes para todo el mercado interior, con ayuda del principio de la armonización plena. Además esta Directiva está destinada a regular el comercio electrónico con participación de consumidores, dado que esta forma de contratar es cada vez más popular y permite perfeccionar transacciones transfronterizas de una manera prácticamente ilimitada.

---

20 European Parliament press release 17.03.2010 http://www.europarl.europa.eu/sides/getDoc.do?language=en&type=IM-PRESS&reference=20100317IPR70798

21 Libro verde sobre la revisión del acervo en materia del consumo...*cit.* pp. 6 -7

Aunque la Directiva adoptada instaura una regla general de armonización plena en su art. 4, la armonización plena se aplica sólo a algunos aspectos de la contratación a distancia y fuera de los establecimientos mercantiles, es decir sobre todo al deber de la información precontractual y al derecho de desistimiento. La armonización plena de estas cuestiones parece justificada. La situación de fragmentación jurídica debida a cuestiones tales como el hecho de la existencia de diferentes plazos para ejercitar el derecho de desistimiento causaba inseguridad, además de causar un aumento de costes en transacciones transfronterizas, y todo ello a pesar de no añadir nada a la mejora de la protección de los consumidores[22].

3.2. La importancia de la Directiva para el comercio electrónico

Las Directivas derogadas, sobre todo la 97/7/CE, ya no correspondían a la realidad social y tecnológica y por lo tanto a las necesidades del mercado común. Es muy importante entender que Internet durante los últimos años se ha convertido en un instrumento de la vida cotidiana de los ciudadanos europeos, no sólo como un instrumento para contactar con los amigos y buscar información, sino también como una herramienta muy poderosa para adquirir bienes y servicios, así como para gestionar negocios. Como el legislador europeo no previó tal evolución, la antigua Directiva relativa a contratos a distancia ya no se adaptaba a la realidad socioeconómica de la Unión Europea.

La Comisión en su Comunicación pone de manifiesto que la nueva Directiva relativa a los derechos de consumidores es hoy en día el principal instrumento de protección de consumidores en el ámbito del comercio electrónico[23]. En el ámbito de aplicación de la Directiva quedan incluidos los bienes de contenido digital (*digital content*), tales como *software*, juegos, música o películas, que por su naturaleza son especialmente aptos para su venta en línea. Es digno de subrayar que la venta de bienes de este tipo no estaba especialmente regulada por las antiguas Directivas. La nueva Directiva regula también la contratación con utilización de subastas *on-line*, cuestión excluida del ámbito de aplicación de las Directivas anteriores.

3.3. Las novedades relativas al comercio electrónico establecidas por la Directiva

La Directiva en su art. 2 apartado 7) define el contrato a distancia como «*todo contrato celebrado entre un comerciante y un consumidor en el marco de un sistema organizado de venta o prestación de servicios a distancia, sin la presencia física simultánea del comerciante y del consumidor, y en el que se han utilizado exclusivamente una o más técnicas de comunicación a distancia hasta el momento en que se celebra el contrato y en la propia celebración del mismo*». Esta definición sin duda abarca la mayoría de contratos que pertenecen al ámbito del comer-

22 Ebers, M. (2010). De la armonización minima a la armonización plena: La propuesta de Directiva sobre derechos de los consumidores, *InDret, 2/2010*, 1-47. pp. 17-18

23 Commission Communication: *A coherent framework for building trust in the Digital Single Market...cit.* p. 9

cio electrónico, celebrados entre comerciantes y consumidores a través de Internet, es decir sobre todo los contratos celebrados a través de la página web del empresario.

En el ámbito del comercio electrónico, la Directiva establece unas nuevas reglas, más claras, para la protección de los consumidores. Como una de las novedades más destacables, cabe señalar el derecho de desistimiento sujeto a la regla de plena armonización (art. 9). El plazo para desistir del contrato celebrado a distancia será 14 días contados a partir de la fecha de entrega del bien en el caso de contratos de venta, y a partir de la celebración del contrato para contratos de servicios. El comerciante tendrá la obligación de informar al consumidor sobre su derecho de desistimiento. En su Anexo I letra A, la Directiva presenta un modelo de carta de información, que los comerciantes podrían utilizar para facilitar a los consumidores información sobre el derecho de desistimiento. La omisión de dicha información, según el art. 10, producirá como efecto la ampliación del plazo para desistir, pudiendo llegar a ser de año. Los consumidores podrán desistir usando el modelo de formulario de desistimiento propuesto por la Directiva en su Anexo I letra B. Conforme a lo dispuesto en el art. 13, en el caso de desistimiento, el comerciante deberá reembolsar todo pago recibido del consumidor, incluidos los costes de entrega, en el plazo de 14 días. Además el comerciante tendrá que asumir los costes de devolución del bien si no informa al consumidor de que le corresponderá abonarlos.

En los contratos realizados a distancia los empresarios serán obligados a remitir a los consumidores una serie de informaciones precontractuales acerca del precio completo del bien y servicio (art. 6.1 e), sus características (art. 6.1 a) y además sobre los datos de indetificación del comerciante (art.6.1 b y c). La obligación del empresario de exponer el precio completo significará que el consumidor mientras contrate *on-line,* tendrá que conocer el precio total del bien o servicio antes de hacer un pedido. Es decir, no podrá aparecer ningún coste adicional después de entrar en el formulario de pedido. Como dispone art. 8.2, el consumidor deberá estar claramente informado de que la realización del pedido implica una obligación de pago. Además el comerciante tendrá que señalar los costes de devolución del bien en el caso de la ejecución del derecho de desistimiento (art.6.1 i). Conforme a lo dispuesto en el art. 22, el comerciante será obligado a obtener el consentimiento expreso del consumidor para todo pago adicional a la remuneración acordada para la obligación principal. Esto significa que el consentimiento prestado a través de las opciones por defecto (*pre-ticked boxes*) que el consumidor debe rechazar para evitar el pago adicional no será válido. También en el caso de servicios adicionales llamados a menudo «gratuitos» los comerciantes deberán asegurar que los consumidores entienden el precio real de tales servicios. Además, no se podrán cobrar tasas que superen costes realmente alcanzados por utilización de determinados medios de pago (art. 19). Esta norma tiene transcendencia sobre todo para pagos realizados en línea con empleo de tarjetas de crédito.

La Directiva regula también las cuestiones relativas a los contratos de suministro de contenido digital *(digital products*). Explica que por contenido digital se entiende los datos producidos y suministrados en forma electrónica, independientemente de si se accede a ellos a través de descarga, de emisión en tiempo real o de un soporte material tal como un CD (Considerando (19)). Conforme al art. 6.1, apartados r) y s), los comerciantes tendrán que

facilitar a los consumidores toda información relevante a la funcionalidad del contenido digital y su interoperatividad con los programas conocidos por el comerciante. Los vendedores deberán dar a conocer las restricciones de uso relativas a programas, música o películas ofrecidas con anterioridad a la adquisición de tal bien por el consumidor.

Hay que tener en cuenta que algunas otras directivas, como la Directiva 2000/31/CE (llamada Directiva sobre el comercio electrónico), también establecen normas relativas al comercio electrónico. La Directiva analizada dispone que los requisitos de información que establece serán adicionales a requisitos previstos por la Directiva sobre el comercio electrónico. Sin embargo, en el caso de conflicto de disposiciones relativas al contenido o al modo de proporcionar la información, prevalecerá la disposición de la Directiva 2011/83/UE (art. 6.8 segundo párrafo).

4. CONSECUENCIAS DE LA DIRECTIVA PARA EL COMERCIO ELECTRÓNICO

4.1. Quién se verá afectado por la Directiva

La Directiva 2011/83/UE hace referencia a la protección de los consumidores. Regula las relaciones contractuales entre los profesionales, es decir comerciantes, y consumidores. Entiende por consumidor, según el art. 1, apartado 1), toda persona física que actúe con un propósito ajeno a su actividad comercial, empresa, oficio o profesión. El comerciante está definido en el art. 1, apartado 2) como toda persona física o jurídica, ya sea privada o pública, que actúe con un propósito relacionado con su actividad comercial, empresa, oficio o profesión.

La Directiva regula, a través de su transposición en el derecho interno de Estados Miembros, las relaciones contractuales entre los consumidores y comerciantes. En el caso de las relaciones transfronterizas habrá que analizar en cada caso concreto el derecho aplicable al contrato. Sin entrar en detalles, es necesario decir que el derecho aplicable a los contratos con consumidores está determinado por el Reglamento Roma I. Este acto normativo en su art. 6 establece que la ley aplicable será la ley del país en el que el consumidor tenga su residencia habitual, siempre que el profesional ejerza sus actividades comerciales o profesionales en dicho país o, por cualquier medio dirija estas actividades a ese o a distintos países, incluido el mismo, y el contrato estuviera comprendido en el ámbito de dichas actividades. Esta normativa está vigente en todos los Estados Miembros, salvo en Dinamarca. Si el comerciante no dirige sus actividades hacia el país del consumidor, será aplicable el art. 4 del Reglamento que determina la aplicación de la ley de país de la residencia habitual del comerciante. En el caso de contratos realizados *on-line* con empresarios que actúan desde fuera de la Unión Europea será aplicable el derecho internacional privado. La Directiva será entonces principalmente aplicable a las relaciones contractuales entre los consumidores y empresarios europeos.

4.2. Derechos acordados a los consumidores

Reconoce nuevos derechos a los consumidores que quieran adquirir los bienes y servicios en línea. Sin duda unas reglas más claras y unificadas acerca del derecho de de-

sistimiento resultarán provechosas para los consumidores. Asimismo parecen beneficiosas desde el punto de vista de los consumidores, las normas sobre la información precontractual que les deberán facilitar los comerciantes. Claramente no se puede adquirir bienes a través de Internet sin conocer sus principales características. Igualmente la información relevante al comerciante parece apropiada. Sin embargo, hay que tener en cuenta que las exigencias sobre información precontractual de la Directiva analizada están completadas por otros actos normativos. Así, surge la pregunta de si el consumidor realmente podrá asimilar tanta cantidad de información. En realidad, los consumidores no leen toda la información facilitada, igualmente como no leen las condiciones generales de contratación[24]. Los consumidores eligen los bienes y servicios y toman decisiones en función de sus necesidades y del precio, sin prestar atención a la información precontractual o condiciones generales de contratación. La información les sería útil a los consumidores a la ahora del incumplimiento por parte del comerciante, para comprobar cómo debería haber sido el producto y cuáles fueron las cláusulas del contrato. Por lo tanto, parece apropiada la exigencia de proporcionar al consumidor toda la información precontractual, así como las condiciones generales de contratación, en un soporte duradero para que consumidor guarde la información durante el tiempo necesario (art. 8.7). La información precontractual tiene entonces mayor trascendencia para el periodo después de celebración del contrato. La Directiva en su art. 8.4 tiene en cuenta ese problema en aquellos casos en donde la técnica de comunicación a distancia en que el espacio (o el tiempo) para facilitar la información son limitados, como por ejemplo en el caso de acceder a Internet utilizando un teléfono móvil. En este caso el comerciante estará obligado a facilitar al consumidor sólo un mínimo indispensable de la información precontractual, las demás informaciones podrán ser proporcionadas después.

Muy favorables para los consumidores serán las nuevas normas que regulan los aspectos de la contratación en línea vinculados con los costes. Esto abarca no sólo el coste de adquisición del bien o servicio mismo, sino también todos los posibles pagos adicionales. Los consumidores serán informados sobre el precio completo, las modalidades de pago aceptadas y las tasas por utilización de determinados medios de pago. Los comerciantes les facilitarán igualmente la indicación del máximo coste posible que supondría la devolución del bien. Además, los consumidores deberán confirmar expresamente todos los pagos adicionales. Conociendo el precio completo y el importe total que deberían abonar, los consumidores podrán tomar las decisiones más consientes sobre sus compras en línea. Gracias a estas reglas las compras a través de Internet se convertirán en un modo de adquirir bienes y contratar servicios mucho más fácil, seguro y probablemente más habitual.

En cuanto a las posibles desventajas de la Directiva, desde el punto de vista de los consumidores, la regla de la armonización plena tiene mucha transcendencia. La armonización

24 Así amplia doctrina sobre condiciones generales de contratación, por ejemplo: Alfaro Aguila-Real, J. (2008). El control de la adecuación entre precio y prestación en el ámbito del derecho de las cláusulas predispuestas. *I Foro de Encuentro de Jueces y Profesores de Derecho Mercantil. Barcelona 2008. Materiales.* http://www.upf.edu/eventia/08/mercantil/pdf/Adecuacion_precio_prestacion_J_Alfaro.pdf

puede contribuir a la disminución del nivel de protección para los consumidores en algunos Estados Miembros, donde la normativa vigente es más favorable que las reglas establecidas por la Directiva.

4.3. La situación de empresas bajo la nueva normativa

La Directiva está destinada no sólo a proteger a los consumidores, sino también a mejorar el funcionamiento del mercado interior. Esto implica igualmente un avance en la situación de los comerciantes que actúan en el ámbito electrónico. Ciertamente, la Directiva supone muchas ventajas para los empresarios. En primer lugar la unificación de algunas normas generará más claridad y previsibilidad en las relaciones contractuales domésticas y transfronterizas. También la posibilidad de utilización de los modelos de cartas de información sobre el derecho de desistimiento facilitará para los comerciantes el cumplimiento del deber de información precontractual.

Asimismo es de esperar que la nueva Directiva traiga consigo un incremento en cuanto al nivel de conocimientos de los empresarios acerca de las normas vigentes. Los estudios demuestran que hoy en día solamente el 29% de los comerciantes saben dónde buscar información o asesoramiento acerca de la normativa relativa a la protección de los consumidores vigente en otros Estados Miembros y hasta el 72% no conoce el plazo otorgado, en sus países, a los consumidores para ejercer el derecho de desistimiento[25]. Los debates acerca de la Directiva, sin duda, contribuirán al aumento de interés y por tanto el conocimiento de los comerciantes que actúan en el ámbito electrónico.

Sin embargo, parece que la Directiva, más que nada, sobrecarga a los comerciantes de nuevas obligaciones. Seguramente aumentará la cantidad de informaciones precontractuales que habrá que facilitar a los consumidores. El derecho de desistimiento otorgado a los consumidores y sus características también pueden resultar perjudiciales para los empresarios. En primer lugar está la obligación de reembolsar al consumidor, en el caso de su desistimiento, todos los costes del bien o servicio, incluso los costes de la entrega, cuestión que es muy desfavorable para los comerciantes. Aparte de eso, si el comerciante no informa al consumidor claramente que este debería abonar los costes de la devolución del bien, también incumbirá al empresario cubrir estos gastos. Hoy en día ya numerosos comerciantes ofrecen la entrega del bien gratuita, o mejor dicho incluida en el precio y por lo tanto, en el caso de devolución, reembolsan también su valor. Sin embargo otros empresarios no podrán permitirse abonar estos costes en el caso de desistimiento. No obstante, los consumidores, conscientes de que en el caso de desistimiento se les reembolsará sólo el precio del bien sin gastos de su entrega, todavía siguen comprando de estos empresarios. Surge la pregunta si ¿el mercado no puede autorregularse hasta un cierto punto? Además, en la época de la crisis, es necesario promover

25 Flash Eurobarometer 300, retailers' attitudes towards cross-border trade and consumer protection, 2011 en: Commission Communication: *A coherent framework for building trust in the Digital Single Market...cit.* p.8

la actividad económica y el comercio, teniendo en cuenta que demasiada regulación y proteccionismo no contribuyen al sostenimiento de la economía[26].

Asimismo parece desequilibrada la normativa relativa al plazo de reembolso de todo pago recibido del consumidor. El comerciante deberá reembolsar estos costes al consumidor antes de que hayan transcurrido 14 días desde que ha sido informado del ejercicio del derecho de desistimiento por el consumidor. El consumidor tendrá que efectuar la devolución del bien en el mismo plazo. Por consiguiente, podría ser que el comerciante tendría que reembolsar los pagos antes de tener la ocasión de comprobar el estado del bien. Los comerciantes deberán asumir los costes más elevados de la ejecución del derecho de desistimiento por el consumidor. Como consecuencia de lo expuesto anteriormente, la Directiva causará el incremento del riesgo financiero de las empresas presentes en el ámbito electrónico.

4.4. La recepción de la Directiva por los Estados Miembros

Para los Estados Miembros, sin duda, la cuestión más controvertida vinculada con la nueva Directiva es la regla de armonización plena. Ante todo, los Estados Miembros de la Unión, provenientes de diferentes tradiciones y culturas jurídicas, aceptan la armonización del derecho sólo hasta un cierto punto. No obstante, el principio de la armonización mínima siempre deja un margen de libertad para poder establecer las normas más adecuadas a la realidad socioeconómica de cada Estado. La regla de armonización plena privará los Estados de la posibilidad de actuar conforme a sus necesidades internas[27]. La regla de la armonización plena en la Directiva está bastante restringida, sin embargo tendrá importancia por lo que respecta a la información precontractual y al derecho de desistimiento.

5. CONCLUSIONES

La nueva Directiva 2011/83/UE tiene mucha transcendencia para el comercio electrónico. Destinada a la protección de los consumidores y a la eliminación de los obstáculos que impiden el correcto funcionamiento del mercado interior constituye sin duda un paso adelante en la armonización del derecho de contratos. Cabe destacar que el logro de sus fines dependerá también de la transposición de sus normas al derecho interior de los Estados Miembros. La armonización plena podrá eliminar la fragmentación jurídica de las normas sólo si la interpretación de ellas llega a ser semejante en todos los Estados Miembros de la Unión Europea.

El desarrollo del comercio electrónico, de naturaleza transfronterizo, podría contribuir a la integración europea y a la creación del mercado interior sin obstáculos. Igualmente provocaría unos beneficios para los consumidores, tales como precios más bajos, más opciones, mejora de la calidad de bienes y servicios. También los comerciantes se aprovecharían de ello

26 Berenguer Gimenéz, L. (2010) El derecho de la competencia en un marco de crisis global, *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche, 1(6),* 1-12. p.4

27 Ebers, M. (2010). De la armonización minima a la armonización plena...*cit.* p.12

al acceder a nuevos mercados donde podrían encontrar más clientes[28]. Sin embargo, la nueva Directiva introduce muchas reglas controvertidas que podrían incluso ralentizar el desarrollo del comercio electrónico nacional y transfronterizo en el mercado europeo. Los comerciantes, a quienes se les han asignado demasiadas obligaciones tales como la información precontractual o las obligaciones vinculadas con el ejercicio del derecho de desistimiento por los consumidores, subirán los precios de bienes y servicios. En consecuencia, los consumidores deberán pagar su propia protección.

La Directiva sobre los derechos de consumidores constituye un tipo de compromiso entre la Propuesta inicial que seguía la visión de la Comisión sobre el futuro del derecho del consumo y, más extensamente, derecho de contratos, y por otro, las ideas que intentó introducir el Parlamento Europeo y el Consejo. La Comisión propuso la armonización plena como remedio a los obstáculos para el funcionamiento del comercio transfronterizo, sin embargo este concepto fue ampliamente criticado. Por lo tanto, la Comisión sigue buscando otras soluciones para mejorar el funcionamiento del mercado interior[29].

Hay que tener en cuenta también que el Libro verde sobre la revisión del acervo en materia de consumo fue adoptado por la Comisión a principios del año 2007 y la Directiva misma fue propuesta en el año 2008. Por lo que al no haberse previsto el posible alcance de la crisis en Europa, la Propuesta no ha sido adecuada a la situación económica actual, a pesar de los cambios introducidos durante el proceso de adopción de la Directiva, su carácter parece un poco anticuado. Demasiada regulación provoca ralentización del mercado, que conlleva un efecto indeseable en épocas de crisis.

6. BIBLIOGRAFÍA

Alfaro Aguila-Real, J. (2008). El control de la adecuación entre precio y prestación en el ámbito del derecho de las cláusulas predispuestas. *I Foro de Encuentro de Jueces y Profesores de Derecho Mercantil. Barcelona 2008.Materiales.* http://www.upf.edu/eventia/08/mercantil/pdf/Adecuacion_precio_prestacion_J_Alfaro.pdf

Aubert de Vincelles, C. (2011). Perspectives for European Consumer Law. Towards a Directive on Consumer Rights and Beyond, H. Schulte-Nölke and L. Tichy (eds), Sellier, 2010: Book Review. *European Review of Contract Law, 4/2011*, 567-572

Berenguer Gimenéz, L. (2010) El derecho de la competencia en un marco de crisis global. *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche, 1*(6), 1-12

Commission Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A coherent framework

28 Commission Communication: *A coherent framework for building trust in the Digital Single Market...cit.* p. 3

29 Reich, N. (2012). EU Strategies in Finding the Optimal Consumer Law Instrument. *European Review of Contract Law, 1/2012,* 1-29. pp.2-3

for building trust in the Digital Single Market for e-commerce and online services. COM(2011) 942

Commission Staff Working Paper: Report on the Outcome of the Public Consultations on the Green Paper on the Review of the Consumer Aquis http://ec.europa.eu/consumers/cons_int/safe_shop/acquis/acquis_working_doc.pdf

Cruz Rivero, D. (2009). Contratación electrónica con consumidores. *Revista de la contratación electrónica, 109-2009*, 3-42

Deshayes, O. (2011) Réponse du LEJEP au Livre vert de la Commission européenne http://ec.europa.eu/justice/news/consulting_public/0052/contributions/91_fr.pdf

Ebers, M. (2010). De la armonización minima a la armonización plena: La propuesta de Directiva sobre derechos de los consumidores, *InDret, 2/2010*, 1-47

Estrategia comunitaria en materia de política de los consumidores 2007-2013, Luxemburgo 2007 http://ec.europa.eu/consumers/overview/cons_policy/doc/cps_0713_es.pdf

European industry associations open letter http://www.e-commercefacts.com/news/2011/05/branch-organisations-cons/index.xml

European Parliament press release 17.03.2010 http://www.europarl.europa.eu/sides/getDoc.do?language=en&type=IM-PRESS&reference=20100317IPR70798

Grundmann, S. (2011). The Future of Contract Law. *European Review of Contract Law, 4/2011*, 490-527

Hesselink, M. W. (2009). The Consumer Rights Directive and the CFR: two worlds apart?, *European Review of Contract Law, 3/2009*, 290-303

Howells, G., Reich, E. N. (2010) Extent of Harmonisation in Consumer Contract Law. Note on the level of harmonization. *European Parliament. Directorate General for Internal Policies. Policy Department C: Citizens' Rights and Constitutional Affairs. Legal Affairs. PE 432.728* http://www.europarl.europa.eu/studies

Libro verde sobre la revisión del acervo en materia del consumo COM(2006) 744 final

Micklitz, H.-W., Reich, N. (2009) Crónica de una muerte anunciada: The Commission Proposal for a Directive on Consumer Rights, *Common Market Law Review, 46/2009*, 471–519

Propuesta de Directiva del Parlamento Europeo y del Consejo sobre derechos de los consumidores, COM(2008)614 final

Reich, N. (2012). EU Strategies in Finding the Optimal Consumer Law Instrument. *European Review of Contract Law, 1/2012*, 1-29

Schieman, M. (2008). Enterprises by size class – overview of SMEs in the EU. Eurostat. Statistics in focus, 31/2008 http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-08-031/EN/KS-SF-08-031-EN.PDF

Twigg – Flesner, Ch., Metcalfet, D. (2009) The proposed Consumer Rights Directive – less haste, more thought? *European Review of Contract Law, 3/2009*, 368-391

UEAMPE open letter http://www.ueapme.com/IMG/pdf/Letter_to_perm_reps_May_2011.pdf

10

MYTHS AND TRUTHS OF ONLINE GAMBLING

Margaret Carran
City Law School, City University, London, Lecturer

ABSTRACT: The view that online gambling presents increased risks of gambling addiction and increased minors' participation underlies several regulatory approaches and judicial opinions. It has been seen in the justification given by some States for protecting their gambling monopolies or for prohibiting interactive gambling either partially or in entirety and in judicial statements made by the European Court of Justice. The paper challenges the validity of this assumption by analyzing existing literature to evidence the divergence between actual gambling behavior and legislative attitudes. It is undisputed that online gambling presents different issues but the lack of effective dialogue between law and social science knowledge leads to over – reliance by many regulators, to their detriment, on the unverified assumption that online gambling leads to more harm. The analysis of online gambling participation rates, player's demographics and social aspects of cyberspace gaming experience shows that many assumptions are not supported by empirical evidence. Furthermore, Internet's specific capabilities present unique opportunity to minimize gambling related risks more effectively than any mechanisms that can be employed for traditional forms of gambling. An evaluation of under-aged exposure shows that it is the unregulated environment of free gambling that potentially presents particular risks for adolescents.

KEYWORDS: Online gambling, regulation, internet capabilities, cyberspace gaming experience, adolescents.

1. ONLINE GAMBLING IN CONTEXT

1.1. Introduction

The term «online gambling» attracted negative connotation from the early usage of Internet for the purpose of betting, wagering or casino gaming. The attitudes are changing but the negative rhetoric still dominates public debates and underpins several legislative decisions. Proponents of online gambling, who highlight the potential benefits of increased State revenues, wider accessibility for homebound or under-privileged and the general futility of attempting to successfully enforce any prohibition are normally silenced by critics who persuasively point to the increased dangers of social harm and moral decay that are inherently increased by Internet gambling. It is claimed that this further degeneration of social values, over and above those already associated with traditional forms of gambling, results from substantially higher threat of under-aged gambling, increased crime and elevated levels of problem gambling within the population. General public opinion tends to correspond with those perceptions[1] but such attitudes are frequently an extension of the belief that gambling,

1 Wardle, et al. British Prevalence Study 2010. Retrieved March 2012 from www.gamblingcommision.gov.uk The study found that public view of gambling remains more negative than positive.

regardless of form, is immoral and harmful. Most acknowledge that gambling produces economic benefit[2] but some claim that any financial gain is outweighed by the social costs[3]. Yet, a large number of people enjoy gambling as a legitimate recreational activity including those who argue that gambling should be strictly controlled and discouraged. A significant «third-person effect» found to exists for gambling websites[4] and public acceptability of many assertions made by anti-gambling critics may contribute towards the potential explanation of this apparent contradiction.

1.2. Snapshot of legal framework

Online gambling regulatory regimes are very complex and varied due to differing priorities afforded to economic, cultural and social considerations and to the issue of public health by different jurisdictions. Legislative measures range from full prohibition[5], partial prohibition[6], state monopoly[7], liberal regulation[8] to open permission in unregulated environment[9]. However, the varieties of approaches are policy representations of the same aims – the safeguard of vulnerable people, consumer protection and minimisation of crime. Islamic countries have historically banned all forms of gambling regardless of the medium of delivery due to it being explicitly prohibited by Koran[10]; some States permit both types equally and some regulatory regimes treat both forms differently. In Australia offline gambling is legal for adults and can be provided by any commercial enterprise licensed and controlled by the ACT Gambling and Racing Commission[11]. Online gambling by punters is not prohibited but the Interactive Gambling Act 2001 criminalised the offering and advertising of online casino games to those who are physically located in Australia[12] or in any designated

2 Kearney,M.S.(2005). The Economic Winners and Losers of Legalized Gambling. *National Tax Journal, Vol. LVIII, No. 2.*

3 Jawad,C & Griffiths,S.(2010). Taming the casino dragon. *Community, Work & Family, Vol.13, No.3, pp.329-347* citing Grinols (2004) who claims that every $46 in economic benefit causes social costs of up to $289 due to elevated crime rates, financial losses and loss of productivity in the workplace. This estimate is disputed.

4 Fang,W & Seounmi,Y.(2004). Motivation to Regulate Online Gambling and Violent Game Sites: An Account of the Third-Person Effect. *Journal of Interactive Advertising, Vol.4, Issue 3 pN.PAG.*

5 E.g. Saudi Arabia

6 E.g. United States or Australia

7 E.g. Portugal

8 E.g. United Kingdom

9 There are very few states that offer a truly unregulated market but it can be argued that some jurisdictions provide only token regulations.

10 Binde,P.(2005). Gambling Across Culture: Mapping Worldwide Occurrence and Learning from Ethnographic Comparison. *International Gambling Studies, 5:1m, pp.1-27*

11 Established under the Gambling and Racing Control Act 1999 (Australia)

12 S.15.

country.[13] Online wagering on sports events is legal with the exception of betting on live events that have already commenced. Recent recommendation of the Productivity Commission Inquiry Report on Gambling 2010 which suggested liberalization of online gambling regulation was met with a strong opposition from the Australian Government who argued that «*… the Internet is very attractive to this group [problem gamblers] and, though the evidence is weak, gambling online may exacerbate already hazardous behaviour*»[14]. The prohibited activities were singled out because of their perceived highly addictive characteristics but the regulation created a rather paradoxical outcome whereby Australian businesses can continue to offer their gambling services but only to overseas clients[15] but their residents wishing to gamble online need to seek providers from within foreign jurisdictions that are willing to ignore Australian laws[16] and are likely to be unregulated. From social perspective, their legal position could cynically be described at attempting to import gambling revenues while exporting the costs. United States also differentiate between online and offline gambling. Both are largely regulated by individual States but on federal level the Unlawful Internet Gambling Enforcement Act 2006 created a federal offence of «*knowingly accepting monies by anyone in the business of betting and wagering in connection with the participation of another person in unlawful internet gambling*».[17] The Act does not substantively define «unlawful internet gambling» term but the federal aim is clear. The law intends to eradicate online gambling provided by offshore operators by making the provision of such facilities illegal and anyone found in contravention can be arrested and their assets seized. US's claim that their wish to eliminate online gambling due to its perceived higher dangers[18] is undermined by two exceptions. The Interstate Horseracing Act 1978 arguably[19] continues to legalize online betting on horse racing provided this is permitted by the State where the bet is placed and the State where the race actually occurs. Secondly, the Gaming Regulatory Act (IGRA) grants exclusive jurisdiction to Indian tribes to regulate all gambling, implicitly including interactive gaming, on their native territories. The exceptions produce some peculiar anomalies. E.g. in the State of Washington online gambling is a serious crime (equivalent to third

13 S.15A. Designated countries may be nominated in writing by the relevant minister but only upon request and only when reciprocal arrangements exist.

14 Jarrod,J.(2011). The Safest Bet: Revisiting the Regulation of Internet Gambling in Australia. *Gaming Law Review and Economics, Vol.15, Number 7/8, pp.441-453*

15 Smith,A.D. & Rupp,W.T.(2005) Service Marketing Aspects Associated with the Allure of E-Gambling. *Services Marketing Quarterly, Vol.26(3) pp.83-103*

16 Offshore providers face the same prohibition but enforcement is difficult.

17 Dayanim,B.(2007). Internet Gambling Under Siege. *Gaming Law Review, Vol.11, No.5, pp.536-550*

18 As opposed to just protecting US' revenues.

19 The actual legal position is debated and contrary views are presented within the literature. See Ian Abovits «Why the United States should rethink its legal approach to Internet gambling: a comparative analysis of regulatory models that have been successfully implemented in foreign jurisdictions», 22 Temp, Int'l & Comp. L.J.437, 2007 p.448 and the Fact Sheet about UIGEA 2006, retrieved March from www.casinoaffiliateprograms.com/UIGEA.Fact_sheet.pdf for contradictory views.

degree rape) when at the same time the State hosts 28[20] land based casinos under Indian's governance. Those inconsistencies justified WTO's ruling against US in the trade dispute with Antigua which alleged that the total prohibition of the supply of online gambling unjustifiably infringed the free trade agreement under the GATT provisions. However; WTO endorsed the view that Internet is inherently more dangerous and would have permitted this as an objectively valid justification for restricting trade but for the inconsistency in US' legal regime[21]. Similar endorsement was given by the European Court of Justice in Bwin v Santa Casa da Misericordia de Lisboa[22] and Zeturf v Premier Ministre[23]. Within Europe the attitudes are more liberal and increasingly States realize that regulating online gambling is more effective than attempting to enforce prohibition. France and Italy have recently relaxed their monopolies and allow licensed commercial enterprises to enter their market. In United Kingdom online gambling can be offered by commercial businesses on a competitive basis subject only to the possession of a valid remote operating and personal license granted by the Gambling Commission which is responsible for ensuring that gambling is crime-free, fair to punters and that those who are particularly at risk are not permitted to participate. It is submitted that only strict and consistent regulation has the realistic prospect of minimizing gambling related harm. Lack of regulation allows unscrupulous entities to exploit vulnerable customers but experience from US and Australia shows that prohibition drives customers to unregulated offshore websites; a position not undermined by the widely publicized few arrests successfully made by US[24] authorities.

2. MYTHS AND TRUTHS OF THE INTERNET GAMBLING

It is perceived that online environment presents unique experience that presents a higher risk of gambling addiction which in turn leads to the increased social and economic costs. The Internet features that are argued to increase those dangers can broadly be grouped into three categories: (1) omnipresence of gambling website with 24 hours access; (2) unique online gaming experience and (3) gambling by under-aged. Further claims regarding extra-territorial enforcement difficulties and increased risks of fraud are outside the scope of this paper. The article does not intend to convince the reader that online gambling does not pose risks; rather it intends to show that the risks may not necessarily be more likely that those normally associated with traditional forms of gambling. Furthermore, it intends to show

20 As of 2003

21 Dilimatis, P.(2011). Protecting public morals in a digital age: revisiting the TWO rulings in US-Gambling and China-Publications and AudioVisual Products. *Journal of Economic Law, 14(2), pp.257-293*

22 Case C-42/07, judgment of 8 Sept 2009, Lexis.

23 Case C-212/08, [2008] 1 CLRM 4.

24 Hornle,J and Zammit,B. (2010). Cross- border Online Gambling Law and Policy (1st ed.). London: Edward Elgar Publishing Limited.

that the Internet's unique features, if effectively utilized, could render online gambling a safer experience.

2.1. Omnipresence of online gambling

The prediction, based on the opportunity theory, that widespread accessibility of online gambling sites will increase overall participation rates and introduce newcomers to gambling, has not at yet fully materialized. United Kingdom permitted online gambling effectively since its inception and remote facilities can now be offered by any licensed commercial enterprise. The requisite licenses are granted by the Gambling Commission only after it is satisfied that the applicant is of sufficient probity, will comply with social responsibilities' codes and offers adequately tested and fair equipment. The Commission is, however, not permitted to apply a demand test which has led to a proliferation of UK based gambling websites.[25] Internet is opened 24 hours from the comfort of individual's home and with the estimated 2332 total number of gambling websites worldwide[26] the potential to participate seemingly never ends. This increased offering has not caused the feared rush towards online gambling. The absolute participation rates are increasing but the growth in number of online players seems slower than the comparable growth in traditional forms. The British Prevalence Study, most recently conducted in 2010 show a modest comparable 1% increase in online participation rates from 2007 (6% in 2007 to 7% in 2010).[27] The number of people who placed bets online dropped from 4% to 3% but this was counterbalanced by the increase in those who played on online casinos, bingo and slot machines or using a betting exchange. Online participation can be contrasted with the prevalence rates in all other traditional forms of gambling (excluding lottery) which increased by 8% from 48% in 2007 to 57% in 2010. This disparity can no longer be attributed to the relative newness of Internet or unspecified fear of transacting online. Across Europe on average 70% of households have broadband Internet access at home[28] and the penetration rates are increasing daily. Many have access at work, schools or from cybercafés. In UK, in the first three months of 2010 more than 51% of people aged over 15 shopped online. In Australia the Productivity Commission estimated that there were only between 1 and 4% of Australians who gambled online in 2010 but this statistic was challenged by Blaszczynsky and Gainsbury[29]. They cited results from the nationally representative Roy Morgan Research which indicated that 30%

25 297 operators possessed license for remote gambling as of September 2010.

26 Retrieved in March 2012 from *http://gambling.addictionblog.org* – no actual numbers available and estimates vary.

27 Excluding purchase of online lottery ticket only.

28 Eurostat Statistics Explained; Information society statistics at regional level, European Commission. Retrievd in March 2012 from *http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Information_society_statistics_at_regional_level*

29 Gainsbury,S & Blaszczynky,A.(2010). Address to Senate Community Affairs Committee: The Prevalence of online and interactive gambling in Australia, Retrieved, March 2012 from *https://senate.aph.gov.au/submissions/.../viewdocument.aspx?id*

of those over the age of 16 gambled online. The true figure probably lies somewhere between those two but the figures demonstrate that the illegality or restricted availability does not per se suppress demands. Unlike offline gambling the commencement of online betting does not easily starts on an impulse. In UK there is a significant high street presence of land based casinos and betting shops and everyday exposure is unavoidable. This, coupled with the removal of 24-hour cooling off period[30], easy age-verification and the potential to instantly play and immediately collect any winnings in land based venues may increase spontaneous entry. Virtually the individual punter must make a positive decision to seek a gambling website, download the relevant software and register with their personal and payment details. Although most websites allow playing instantly after the registration, the ability to collect any potential winning must be delayed after age-verification procedures have been carried out. This slows the whole process down and minimizes the risk of impulsive commencement of online gambling.

2.2. Problem gambling

Several studies concluded that those who gamble online are at higher risks of developing gambling related problems that those who do so only offline. Problem gambling can be measured by several screens but the most commonly used are: DSM-IV, PGDI and South Oaks Gambling Screen. Welte et al[31] found that the odds of risk of developing gambling problems increases by 90% if a casino is opened within 10 mile radius from individual's residence. By analogy the invention of online casino reduces this distance to 0 for the vast majority of household. The British Prevalence Study, using DSM-IV, measured the level of overall problem gambling to be 0.9%. This represented an increase of 0.4% from 2007 and 1999 where the level of problem gambling was measured at 0.6% in both years[32]. With regards to compulsive gambling exclusively amongst online players Griffiths et al[33] reported rate of 5%. Wood et al[34] focusing on online poker reported that 18% of the sample displayed symptoms of experiencing gambling harm; Wood and Williams[35] found that in a self-selected group of online North American gamblers 43% satisfied the criteria for moderate or severe gambling problems. Although most of those studies[36] can be criticized for using convenience samples that may

30 Prior to the Gambling Act 2005 casino players had to register 24 hours before gambling.

31 Welte et al, 2004 cited in Jawad et al, Ibid, ref.3.

32 The differences resulted in the p value of 0.046 (at the margin of statistical significance) which could be due to random fluctuation or due to an upward trend in problem gambling.

33 Griffiths,M; Wardle,H; Orford,J; Sproston,K and Erens,B.(2009). Rapid Communication: Socio-demographic Correlates of Internet Gambling: Findings from the 2007 British Gambling Prevalence Survey. *Cyberpsychology & Behaviour, Vol.12, No.2.* There is no equivalent analysis for 2010 statistics.

34 Wood,R.T.A; Griffiths,M; Parke,J.(2007). Acquisition, development, and maintenance of online poker playing in a student sample. *Cyberpsychology & Behaviour, Vol. 10 pp. 354-361*

35 Wood RTA, Williams, RJ.(2007) Problem gambling on the Internet: implication for Internet gambling policy in North America. *New Media & Society 9: pp.520-542*

36 Excluding Griffiths et al, ref.33

have produced biased results there is no merit in challenging their accuracy. Rather, what is disputable is whether the comparison made with rates of offline problem gambling is appropriate. It is argued that the general statistics severely underestimate the actual levels of problem gambling within the general population[37]. All available screens rely on self-reports based on subjective self-assessment of the severity of experienced difficulties which can produce many false negatives. Gambling addiction does not display easy-to-observe physical symptoms. This allows problems to be hidden for a prolonged period of time and those gamblers may trivialize their issues. Discussions with self-confessed problem gamblers showed that «*only 29% said they would have responded to a survey honestly; one-third said they would have concealed the problem, and some 24% said they would have refused to answer the survey*»[38]. Nevertheless, the level of online problem gambling deserves attention regardless of comparability with offline data. Socio-demographic profile of online players, although divergent, is unlikely to explain potentially higher levels of problem gambling. Studies[39] indicate that online players tend to be younger (under the age of either 34 or 40) and at least college educated holding professional and managerial jobs. This does not offer complete match to the profile of a typical problem gambler (also under the age of 35 but with low educational attainment and low income)[40]. If the pathological gambling is indeed higher online the reasons must be different.

2.3. Online gaming experience

The seductive appeal of online gambling and its propensity to cause more additions are stated to be due to the salient factors listed by Griffiths et al[41] [42] that includes: anonymity, escape, immersion, event frequency, associability and «suspension of judgment» due to currency intangibility.[43] [44] Unscrupulous operators may use telescopic windows where, upon ending one session, a player is met with another website usually offering hard-to-refuse, attractive promo-

37 Doughney,J.(2006). Lies, Damned Lies and «Problem Gambling» Prevalence Rates: The Example of Victoria, Australia. *Journal of Business Systems, Governance and Ethics, Vol.2, No.1*

38 Ibid, ref. 37 citing McMillen and Marshall, pp.87-8; citing Banks 2002.

39 Ibid, ref. 33

40 Ranade,S; Bailey.S & Harvey,A. (2006). DCMS: A literature review and survey of Statistical Sources on Remote Gambling, Final Report V1.0. Retrieved in October 2011 from http://kharkiv.academia.edu/AlKOv/Papers/1175157/A_literature_review_and_survey_of_statistical_sources_on_remote_gambling

41 Griffiths,M; Parke,A; Wood,R; Parke,J.(2005). Internet Gambling: An Overview of Psychosocial Impacts. *UNLV Gaming Research and Review Journal, Vol.10, Issue 1 pp.27-39*

42 Griffiths,M.(2003). Internet Gambling: Issues, Concerns and Recommendations. *CyberPsychology & Behavior, Vol.6, No.6, pp.557-568*

43 Valentine,G and Hughes,K.(2009). New Form of Participation: Problem Internet Gambling and the Role of the Family. Retrieved in October 2012 from www.lssi.leeds.ac.uk/projects/5.

44 Fogel, J.(2011). Consumers and Internet Gambling: Advertisement in Spam Emails. *Romanian Journal of Marketing, April 2011*

tional freebies thus enticing further gambling.[45] Targeted advertising with their often misleading glamorization of the prospect of life style changing win[46] and pop up messages[47] were also found to be instrumental in encouraging excessive play. Lack of social interaction is experienced more by online players but many are attracted to this form precisely to avoid contact with strangers[48] and a good proportion gambles online with friends or relatives[49]. Many websites offer interactive features allowing for instant messages or verbal chats between players which the individual can opt to use or disable according to personal preferences. Within the home environment it is easier to hide compulsive gambling but the punter is more likely to be surrounded by non-gambling family members who may be less inhibited to argue and have more incentive to intervene than in a land based casino where individuals are more likely to go either with like – minded friends or alone. The perception of temporary community and social connectedness felt in a casino may actually mask the true nature of the activity. The pressure of other casino goers to make decisions quickly, the encouragement of others to continue playing and the general unwillingness to show distress in public may in fact increase the amount of money spent. Even with the Internet's interactive features, the «disinhibition effect»[50] isolates the players from those tensions. Online gambling does not offer the same glamour, sounds or lights, complimentary drinks or plush high roll rooms as land based casino but online providers work hard to match the experience with 3D colorful graphics, audio-visual stimuli and free bonus incentives. It better facilitates escape and full immersion uninterrupted by other people or by closing times; an aspect particularly attractive to problem gamblers. Further, online and offline casinos exploit people's propensity to see intangible money as less valuable[51]. Land based establishments use chips or tokens and money in online account are converted into credits but the total loss of tangibility of Internet currency makes is more difficult for players to track their spending.[52] The monthly reminder in the form of credit card statement probably comes too late.

2.4. Solution?

However, those internet features could be turned around to be used to manage problem gambling risks better. Online providers already offer many social responsibility measures but

45 Ibid, ref.41.

46 McMullan,J.L & Miller,D.(2009). Wins, Winning and Winners: The Commercial Advertising of Lottery Gambling. *J. Gambling Studies, 25 pp.273-295*

47 Ibid, ref.43

48 Cotte,J & Latour,C.(2009). Blackjack in the Kitchen: Understanding Online versus Casino Gambling. *Journal of Consumer Research, Vol.35, No.5 pp.742-758.*

49 Ibid, ref.43.

50 Suler,J.(2004). The Online Disinhibition Effect. *CyberPsychology & Behavior, Vol.7, No.3, pp321-326*

51 Griffiths,M.(2003). Internet Gambling: Issues, Concerns and Recommendations. *CyberPsychology & Behavior, Vol.6, No.6, pp.557-568*

52 Siemens,J.Ch. & Kopp.S.W.(2011). The Influence of Online Gambling Environments on Self-Control. *Journal of Public Policy & Marketing, Vol.30.(2), pp.279-293.*

those are usually optional and reactive. Contrary to popular assumptions empirical evidence suggests that the solution does not lie with giving players more control functions within the game[53] or with education alone. The latter increases overall understanding but was found not to modify the actual behaviour[54]. Gamblers often join loyalty schemes which allow the operators to use tracking technology[55] to gain better insight of their playing pattern and expenditure than the individual often has himself. Although usually used to offer personalized incentives with the view to increase sales it can be equally effective in reaching the opposite result. All customers should be required to join such a scheme and pop-messages should be displayed at regular and relatively short intervals clearly displaying, in actual currency[56], the amount gambled in the last 24 hours, in the last week and cumulative totals as well as the time played during the same periods and how it compares to the profile of a typical problem gambler. Continuous display of the same data blends with the overall display making it easier to ignore and pop-up messages were found to have generally higher impact on players[57]. If problem gambling is detected telescopic windows, which are difficult to close, could be used to ensure that the player is directed to gambling support websites with information on responsible gambling strategies, diagnostic tests and instant help via chat rooms or messaging service. Such monitoring would never be possible in an offline environment. Imposed breaks should be introduced in a similar way to those already introduced in some games[58] and by placing cookies on the computer the technology could be used to stop players form being able to simultaneously access several sites from the same computer. Instead of relying on voluntary imposition of self-limits operators should be required to run individual checks on each applicants to set individual gambling limits (maximum turnover and maximum losses within a given period) which would be compulsory throughout the game. Such check should not focus just on creditworthiness of the gambler but his overall exposure as between different gambling providers should also be taken into consideration. This would necessitate the creation of a public database (similar to credit referencing system) accessible only by the operators and the player himself but it could be a powerful tool in harm reduction. Compliance with those provisions by all regulated sites would allow customers to easily distinguish

53 Peller,A.J;LaPlante,D.A & Shaffer,H,J.(2008). Parameters for Safer Gambling Behavior: Examining the Empirical Research. *J. Gambling Studies, 24, pp.519-534*

54 Boutin,C; Tremblay,N & Ladoucer,R.(2009). Impact of Visiting and Onsite Casino Information Centre on Perceptions about Randomness and Gambling Behaviours. *J. Gambling Studies, 25, pp.317-330.*

55 E.g. PlayScan designed by Swedish gaming company. Griffiths,M;Wood,R,R,A;Parke,J.(2009). Social Responsibility Tools in Online Gambling: A Survey of Attitudes and Behavior among Interent Gamblers. *CyberPsychology & Behavior, Vol.12, No.4 pp.413-421*

56 Not value of credits.

57 Monaghan, S & Blaczczynski,A.(2010). Impact of Mode of Display and Message Content of Responsible Gambling Signs for Electronic Gaming Machines on Regular Gamblers. *J.Gambling Studies, 26, pp.67-88*

58 E.g. WiiFit; It is acknowledged that the number games with such features is still negligible.

between legitimate and illegitimate sites which would increase their confidence in the former thus benefiting the whole industry.

The solution may be accused of unduly limiting legitimate enjoyment. Framing problem gambling as public health issue[59] increases public acceptability of any restrictions and it is unlikely that those who play recreationally or just for fun would disapprove of such interventions. Those more likely to be annoyed are precisely those they are intended to be helped by those measures. It may also be suggested that the restriction would simply direct players to rogue sites. Undoubtedly, this may be true for some but there is a limit to what the society can do to protect individual from themselves.

3. ADOLESCENTS ONLINE – UNIQUE PROBLEM?

3.1. Prevalence rates

Due to lack of direct contact between the operator and the players online gambling is criticized for its perceived inability to stop under-aged participation. This concern is justified as the risk of potential harm suffered by adolescents is generally agreed to be 3 to 4 times higher than for adults.[60] [61] [62] It is suggested that the «*early onset of gambling participation is the most likely predictor of problem gambling in future*.»[63] Winters et al[64] found that early exposure to gambling environment did not necessarily increase gambling levels in early adulthood but it endorsed the view that gambling problems increase over time thus rendering children particularly vulnerable. Gambling related harm amongst adolescent include feeling guilty, experiencing problems with school work, relationship problems, feeling depressed and suffering from mental anxiety.[65][66] The consequences may be severe as certain outcomes

59 Korn,D; Gibbins,R and Azmier,J.(2003). Framing Public Policy Towards a Public Health Paradigm for Gambling. *J. Gambling Studies, Vol.19, No.2, pp.235-256.*

60 Hayer,T; Griffiths, M and Meyer,G.(2005). Chapter 21: The prevention and treatment of problem gambling in adolescents. In T.P.Gullotta & G. Adams (Eds). Handbook of adolescents' behaviour problems: Evidence-based approaches to prevention and treatment, pp.467-486. New York: Springer

61 Fisher, S.E. (1999) «A prevalence study of gambling and problem gambling in British adolescents», *Addiction Research 7, 509-538*;

62 Hume,M and Mort,G.S.(2011), Fun, Friend, or Foe: Youth Perception and Definitions of Online Gambling; *Social Marketing Quarterly, 17:1, 109-133.*

63 Messerlian,C; Byrne,M.A; Derevensky,J. (2004). Gambling, Youth and the Internet: Should we be concerned?, *The Canadian Child and Adolescent Psychiatry Review, (13):1*

64 Winters,K; Stinchfield,R; Botzet,A & Anderson,N.(2002). A Prospective Study of Youth Gambling Behaviors. *Psychology of Addictive Behaviors, Vol.16, No.1 pp.3-9*

65 Raisamo,S; Halme,J; Murto,A & Lintonen,T.(2012). Gambling – Related Harm Among Adolescents: A Population – Based Study. *J.Gambling Studies* published online 26 February 2012.

66 Barnes et al. (1999). Gambling and Alcohol Use Among Youth: Influences of Demographic, Socialization, and Individual Factors. *Addictive Behaviors, Vol.24, No.6, pp.749-767.*

such as poor education or getting early criminal record are very difficult to rectify. However, the assumption that it is not possible to prevent minors from online gambling for money does not seem to have solid foundation. Arguably online age – verification checks, required by regulators to be carried out before an account can be open and any winnings withdrawn are much more cumbersome for minors to overcome. They involve the need to use a credit card (obtainable generally only by adults), to show valid ID such as passport or driving license and cross-checking the applicant's name and address with credit reference agencies and other public databases. This method is more reliable than reliance on the operator's subjective assessment of the age of a person entering a gambling venue. A mystery shopping exercise carried out in May 2009 by Gambling Commission in UK's offline betting shops produced a staggering 98% rate of non-compliance[67] and shows that direct contact with operators does not guarantee denial of service. Subsequent tests of land based betting shops[68] and adult gaming centres[69] demonstrated excellent improvements but not full compliance. Online, a study by Chambers and Willox[70] which examined 15 most popular sites produced more optimistic results. It found that all operators required actual proof of age[71] before entering and using the site and some of them offered parental controls. Admittedly, none of it will deter a determined youngster from accessing unregulated site or using parents' details but minors' participation rates suggest that this is not such a regular occurrence as may have been originally suggested. Ipsos Mori British Survey of children aged 12 to 15 carried out in 2008-9[72] reported that only 1% of them spent money on online gambling in the seven days preceding the survey despite nearly 96% accessing Internet over the same period while in Quebec Gendron et al[73] identified that only 0.8% of surveyed sample played regularly for money at online casino and 1.9% played online poker.

---

67 Press release «Mystery Shopping tests continue», 31/07/2009. It targeted establishments known for social responsibilities failings.

68 Press release «Under age gambling in betting shops – operators face further tests» 3/12/2009. 74% of Ladbroke betting shops prevented a young person from placing a bet; 68%-William Hill operators, 63%-Tote, 60%-Betfred and 57%-Gala Coral.

69 Press release, «Monitoring under-age gambling in adult gaming centred», 15 June 2010. Out of 57 Talarius Ltd centres visited 41 prevented an under-aged person from gabling; 24 out of 37 for NOL operators and 12 out of 15 for Cashino Gaming Ltd operators.

70 Chambers,C and Willox,C.(2009). Gambling on compliance with the new 2005 Act: Do organisations fulfil new regulations? *International Review of Law, Computers and Technology, Vol.23, No.3 pp.203-215*

71 As opposed to mere confirming the age.

72 British Survey of Children, National Lottery and Gambling. 2008-2009. Retrieved in May 2011 from http://www.natlotcomm.gov.uk/publications-and-research . A small minority of children were aged 11.

73 Gendron A, Brunelle N, Leclerc D, Dufour M, Cousineau M-M.(2009). Comparison of the profiles of young non-gamblers, gamblers and Internet gamblers relative to psychological distress, severity of substance use and impulsiveness/risk taking. 8th Annual Conference Alberta Gaming Res Inst, Banff

3.2. The real danger?

The available statistics seems to suggest that children do gamble but predominantly offline. Either they are not interested in online gambling or more likely the age-verification mechanisms are indeed working. However, this statement is too simplistic. The real danger for adolescents may come in the form of free practice gambling demos and stand-alone gambling games as well as with gambling being incorporated within computer games. Practice sites are proving very attractive to youths and a significant proportion[74] of adolescents use them. Stand-alone gambling games such as poker, roulette or blackjack rated only 12 are available on I-tunes. Unrated casino games are mixed with other children and family's games on popular[75] internet gaming website such as WildTangent. Those games can be tried for free and afterwards children can continue playing either by subscribing to the site or by purchasing game token.[76] Some of those games are clearly targeting young children with the use of children's preferred graphics and music. Gambling activities may also be included as part of otherwise a non-gambling video game. Griffiths[77] uses «Fluff Friends» as an example where girls as young as five enter rabbit racing to win «munny» (sic) that can be used on an in game art. This allows children to learn what gambling means and potentially get attracted to the feel of it before being able to legally gamble or appreciate the potential risks involved. It also normalises the behaviour which may appear to children to be socially acceptable and risk-free and potential misrepresentation of odds of winning may encourage belief that gambling may be a quick way of earning money.[78] Children treat those activities in exactly the way it is presented to them – a mere game played for fun.[79] However, they may not able to understand that the difference between a video game where persistent play improves their skills and allow them to proceed to higher level and gambling where no skills alter chances of success is real.[80/81] Although those ac-

---

Center, Alberta, March 2009 cited in Griffiths, M and Parke, J. (2010) Adolescent gambling on the internet: A review. *International Journal of Adolescents Med Health, Vol.22, No.1, pp.58-75*

74 Ipsos Mori – 24% (ibid, ref.72) – 24%; Gendron (ibid, ref.73) in Quebec – 35%, Byrne in Canada – 43% Byrne, A. (2004) cited in Derevensky J, Gupta, R. (2007) Internet gambling amongst adolescents: A growing concern. *International Journal of Mental Health Addiction, Vol.5, pp.93-101.*

75 Website's shortcut is pre-installed in new computers.

76 Author's own observation.

77 Ibid, ref.73.

78 Gottfried,J.(2004) «The Federal Framework for Internet Gambling», *10 Rich. J.L.&Tech.26, 16* cited in Scoolidge,P.J.(2006) «Gambling Blindfolded: the case for a regulated domain for gambling websites», *Gaming Law Review, Vol.10, No.3.*

79 Ibid, ref. 62

80 Delfabro,P; King,D; Lambos,Ch; Puglies,S.(2009) «Is video game playing factor for pathological gambling in Australian Adolescents», *J.Gambling Studies 25:391-405*

81 Derevensky,J.L; Gupta,R & Magoon,M.(2004) «Adolescent Problem Gambling: Legislative and Policy Decisions», *Gaming Law Review, Vol.8, No.2.*

tivities involve no actual money and there is no empirical evidence that they present actual risk this is an area that should be further explored.

Further, the increased cultural acceptability of gambling causes it to be seen as a family entertainment with minors receiving lottery tickets from parents or other relatives[82] and some players choosing online gambling precisely to enable them to do so with their children[83]. Within the online environment any age-verification attempts would be futile if parents encourage gambling at home. This must be addressed by continuous public education and by raising awareness.

4. CONCLUSION

For the growing number of people Internet is an integral part of their daily life and attempts to stultify technological advances are unmerited and counterproductive. Instead, legislators should harness online capabilities and turn them around to further their policies and protect the general public. However; the effectiveness of any regulation depends on adopting a holistic approach which is the only method that would successfully address such a multifaceted issue like gambling.

5. BIBLIOGRAPHY

Books:

Bogart, W.A.(2011). Permit But Discourage: Regulating Excessive Consumption (1st ed.). London: Oxford University Press.

Hornle,J and Zammit,B. (2010). Cross- border Online Gambling Law and Policy (1st ed.). London: Edward Elgar Publishing Limited.

Miers, D.(2004). Regulating Commercial Gambling (1st ed.). London: Oxford University Press.

Electronic documents/websites:

British Survey of Children, National Lottery and Gambling. 2008-2009. Retrieved in May 2011 from from http://www.natlotcomm.gov.uk/publications-and-research

Eurostat Statistics Explained; Information society statistics at regional level, European Commission. Retrievd in March 2012 from http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Information_society_statistics_at_regional_level

82 Ibid, ref.78

83 Cotte,J & Latour,C.(2009). Blackjack in the Kitchen: Understanding Online versus Casino Gambling. *Journal of Consumer Research, Vol.35, No.5 pp.742-758.*

Gainsbury,S & Blaszczynky,A.(2010). Address to Senate Community Affairs Committee: The Prevalence of online and interactive gambling in Australia. Retrieved in January 2012 from https://senate.aph.gov.au/submissions/.../viewdocument.aspx?id

Gambling Commission Press releases: «Mystery Shopping tests continue», (2009); «Under age gambling in betting shops – operators face further tests», (2009) and «Monitoring under-age gambling in adult gaming centred», (2010). All Retrieved in January 2012 from www.gamblingcommission.gov.uk

http://gambling.addictionblog.org

Ranade,S; Bailey.S & Harvey,A. (2006). DCMS: A literature review and survey of Statistical Sources on Remote Gambling, Final Report V1.0. Retrieved in October 2011 from http://kharkiv.academia.edu/AlKOv/Papers/1175157/A_literature_review_and_survey_of_statistical_sources_on_remote_gambling

UIGEA Fact Sheet 2006. Retrieved in March 2012 from www.casinoaffiliateprograms.com/UIGEA.Fact_sheet.pdf

Valentine,G and Hughes,K.(2009). New Form of Participation: Problem Internet Gambling and the Role of the Family. Retrieved in October 2012 from www.lssi.leeds.ac.uk/projects/5

Book Chapters

Hayer,T; Griffiths, M and Meyer,G.(2005). Chapter 21. The prevention and treatment of problem gambling in adolescents. In T.P.Gullotta & G. Adams (Eds). Handbook of adolescents behaviour problems: Evidence-based approaches to prevention and treatment, pp.467-486. New York:Springer.

Journal Articles

Abovits, I. (2007). Why the United States should rethink its legal approach to Internet gambling: a comparative analysis of regulatory models that have been successfully implemented in foreign jurisdictions», *22 Temp, Int'l & Comp. L. J. 437, p. 448*

Barnes et al. (1999). Gambling and Alcohol Use Among Youth: Influences of Demographic, Socialization, and Individual Factors. *Addictive Behaviors, Vol. 24, No. 6, pp. 749-767.*

Binde, P. (2005). Gambling Across Culture: Mapping Worldwide Occurrence and Learning from Ethnographic Comparison. *International Gambling Studies, 5:1m, pp. 1-27*

Boutin et al (2009). Impact of Visiting and Onsite Casino Information Centre on Perceptions about Randomness and Gambling Behaviours. *J. Gambling Studies, 25, pp. 317-330.*

Chambers, C and Willox, C. (2009). Gambling on compliance with the new 2005 Act: Do organisations fulfil new regulations? *International Review of Law, Computers and Technology, Vol. 23, No. 3 pp. 203-215*

Cotte, J & Latour, C. (2009). Blackjack in the Kitchen: Understanding Online versus Casino Gambling. *Journal of Consumer Research, Vol. 35, No. 5 pp. 742-758.*

Dayanim, B. (2007). Internet Gambling Under Siege. *Gaming Law Review, Vol. 11, No. 5, pp. 536-550*

Delfabro, P; King, D; Lambos, Ch; Puglies, S. (2009) «Is video game playing factor for pathological gambling in Australian Adolescents», *J. Gambling Studies 25:391-405*

Derevensky J, Gupta, R. (2007) Internet gambling amongst adolescents: A growing concern. *International Journal of Mental Health Addiction, Vol. 5, pp. 93-101.*

Derevensky, J. L; Gupta, R & Magoon, M. (2004) «Adolescent Problem Gambling: Legislative and Policy Decisions», *Gaming Law Review, Vol. 8, No. 2.*

Dilimatis, P. (2011). Protecting public morals in a digital age: revisiting the TWO rulings in US-Gambling and China-Publications and AudioVisual Products. *Journal of Economic Law, 14(2), pp. 257-293*

Doughney, James (2006). Lies, Damned Lies and «Problem Gambling» Prevalence Rates: The Example of Victoria, Australia. *Journal of Business Systems, Governance and Ethics, Vol. 2, No. 1*

Fang, Wan and Seounmi, Youn. (2004). Motivation to Regulate Online Gambling and Violent Game Sites: An Account of the Third-Person Effect. *Journal of Interactive Advertising, Vol. 4, Issue 3 pN. PAG.*

Fisher, S. E. (1999) «A prevalence study of gambling and problem gambling in British adolescents», *Addiction Research 7, 509-538;*

Fogel, J. (2011). Consumers and Internet Gambling: Advertisement in Spam Emails. *Romanian Journal of Marketing, April 2011*

Gendron A, Brunelle N, Leclerc D, Dufour M, Cousineau M-M. (2009). Comparison of the profiles of young non-gamblers, gamblers and Internet gamblers relative to psychological distress, severity of substance use and impulsiveness/risk taking. Cited in Griffiths, M and Parke, J. (2010) Adolescent gambling on the internet: A review. *International Journal of Adolescents Med Health, Vol. 22, No. 1, pp. 58-75*

Gottfried, J. (2004) «The Federal Framework for Internet Gambling», *10 Rich. J. L. &Tech. 26, 16* cited in Scoolidge, P. J. (2006) «Gambling Blindfolded: the case for a regulated domain for gambling web-sites», *Gaming Law Review, Vol. 10, No. 3.*

Griffiths et al. (2009). Rapid Communication: Socio-demographic Correlates of Internet Gambling: Findings from the 2007 British Gambling Prevalence Survey. *Cyberpsychology & Behaviour, Vol. 12, No. 2*

Griffiths et al (2005). Internet Gambling: An Overview of Psychosocial Impacts. *UNLV Gaming Research and Review Journal, Vol. 10, Issue 1 pp. 27-39*

Griffiths, M. (2003). Internet Gambling: Issues, Concerns and Recommendations. *CyberPsychology & Behavior, Vol. 6, No. 6, pp. 557-568*

Griffiths et al. (2009). Social Responsibility Tools in Online Gambling: A Survey of Attitudes and Behavior among Interent Gamblers. *CyberPsychology & Behavior, Vol. 12, No. 4 pp. 413-421*

Hoply, A, B. & Nicki, R. M. (2010). Predictive factors of Excessive Online Poker Playing. *Cyberpsychology, Behaviour, and Social Networking, Vol. 13, No. 4 pp. 379-385*

Hume, M and Mort, G. S. (2011), Fun, Friend, or Foe: Youth Perception and Definitions of Online Gambling; *Social Marketing Quarterly, 17:1, 109-133.*

Jarrod, Jolly. (2011). The Safest Bet: Revisiting the Regulation of Internet Gambling in Australia. *Gaming Law Review and Economics, Vol. 15, Number 7/8, pp. 441-453*

Jawad, Caroline and Griffiths, Steve. (2010). Taming the casino dragon. *Community, Work & Family, Vol. 13, No. 3, pp. 329-347.*

Kearney, Mellisa Schettini. (2005), The Economic Winners and Losers of Legalized Gambling. *National Tax Journal, Vol. LVIII, No. 2.*

Korn et al; (2003). Framing Public Policy Towards a Public Health Paradigm for Gambling. *J. Gambling Studies, Vol. 19, No. 2, pp. 235-256.*

Matthews, N; Farnsworth, B; Griffiths, M. (2009). A Pilot Study of Problem Gambling among Student Online Gamblers: Mood States as Predictors of Problematic Behaviour. *CyberPsychology & Behaviour, Vol. 12, No. 6 pp. 741-745*

Messerlian, C; Byrne, M. A; Derevensky, J. (2004). Gambling, Youth and the Internet: Should we be concerned?, *The Canadian Child and Adolescent Psychiatry Review, (13):1*

McMullen, J, L. & Miller, D. (2009). Wins, Winning and Winners: The Commercial Advertising of Lottery Gambling. *Journal of Gambling Studies, 25, pp. 273-295*

Peller, A. J; LaPlante, D. A & Shaffer, H, J. (2008). Parameters for Safer Gambling Behavior: Examining the Empirical Research. *Journal of Gambling Studies, 24, pp. 519-534*

Raisamo, S; Halme, J; Murto, A & Lintonen, T. (2012). Gambling – Related Harm Among Adolescents: A Population – Based Study. *Journal of Gambling Studies. DOI 10. 1007/s10899-0129298-9* published online 26 February 2012.

Siemens, J. Ch. & Kopp. S. W. (2011). The Influence of Online Gambling Environments on Self-Control. *Journal of Public Policy & Marketing, Vol. 30. (2), pp. 279-293.*

Smith, A. D. & Rupp, W. T. (2005) Service Marketing Aspects Associated with the Allure of E-Gambling. *Services Marketing Quarterly, Vol. 26(3) pp. 83-103*

Suler, J. (2004). The Online Disinhibiton Effect. CyberPsychology & Behavior, Vol. 7, No. 3 pp. 321-326.

Welte et al, 2004 cited in Jawad, C and Griffiths, S. (2010). Taming of the casino dragon. *Community, Work & Family, Vol. 13, No. 3 pp. 329-347*

Winters, K; Stinchfield, R; Botzet, A & Anderson, N. (2002). A Prospective Study of Youth Gambling Behaviors. *Psychology of Addictive Behaviors, Vol. 16, No. 1 pp. 3-9*

Wood, R. T. A; Griffiths, M; Parke, J. (2007). Acquisition, development, and maintenance of online poker playing in a student sample. *Cyberpsychology & Behaviour, Vol. 10 pp. 354-361*

Wood RTA, Williams, RJ. (2007) Problem gambling on the Internet: implication for Internet gambling policy in North America. *New Media & Society 9: pp. 520-542*

Xuan, Z & Shaffer, H. (2009). How Do Gamblers End Gambling: Longitudinal Analysis Of Internet Gambling Behaviors Prior to Account Closure Due to Gambling Related Problems. *Journal of Gambling Studies. 25 pp. 239-252.*

LAS NUEVAS TECNOLOGÍAS Y EL BLANQUEO DE CAPITALES: *SECOND LIFE*, ENTRETENIMIENTO ONLINE Y MÉTODO DELICTIVO

Covadonga Mallada Fernández[1]
Doctora en Derecho. Universidad de Oviedo
Estudiante Estudios de Asia Oriental. UOC

RESUMEN: Este trabajo pretende analizar los riesgos de los entornos virtuales y juegos de rol online, como *Second Life* y *World of Warcraft*, los cuales pueden ser utilizados para llevar a cabo delitos tales como el blanqueo de capitales o la financiación del terrorismo ya que en la actualidad, los entornos virtuales no están sujetos a los estrictos controles financieros y los requisitos de intercambio de información del mundo real, por lo tanto, ofrecen una excelente oportunidad para los criminales para llevar a cabo sus actividades ilícitas con impunidad.

Second life es un mundo virtual formado actualmente por más de 9 millones de «residentes» donde no hay leyes ni impuestos. Este mundo virtual tiene su propia moneda, llamada dólar Linden y un producto interno bruto de 500 millones de dólares pero lo más importante es que este dinero ficticio puede convertirse en dólares reales. La escasa regulación normativa del movimiento de capitales dentro de estos entornos virtuales ha hecho que este tipo de organizaciones criminales muevan dólares por todo el planeta virtual para luego convertirlos en dólares reales impunemente. Así, se facilita una plataforma perfecta a los criminales para poder llevar a cabo delitos, tales como el blanqueo de capitales fuera del alcance de las autoridades.

La cuestión no es lo que pasa dentro de SL, que no deja de ser un juego de rol virtual sino que ese dinero es real y tiene consecuencias en la realidad.

PALABRAS CLAVE: Blanqueo de capitales, nuevas tecnologías, financiación del terrorismo, plataformas virtuales, evasión de impuestos.

1. INTRODUCCIÓN

El continuo desarrollo y expansión de Internet como nueva herramienta de comunicación y transmisión de datos lo ha convertido en uno de los medios más utilizado para realizar actividades de carácter lúdico, financiero o comercial. Sin embargo, a la par que esta nueva herramienta se utiliza para llevar a cabo actividades lícitas también se utiliza para otras actividades menos legales que pueden llegar a constituir delitos. Esta *ciberdelincuencia* se aprovecha de la dificultad que tiene la persecución de los delitos en este medio y del anonimato que le ofrece el mismo.

1 Este trabajo ha sido realizado en el marco del Proyecto I+D del Ministerio de Ciencia e Innovación (DER2008-06263) "Una nueva perspectiva tributaria del blanqueo de capitales". Investigadora principal (Dra. Manuela Fernández Junquera).

Aunque los delitos sigan siendo en esencia los mismos que los que se cometen en los medios físicos tradicionales, la peculiaridad de Internet dota a los mismos de una especial estructura que obliga a actualizar los tipos delictivos, los cuales, han sido configurados sobre unos tipos clásicos de relaciones interpersonales, por lo que a partir de ahora se deben modificar las figuras delictivas para adaptarse a estas nuevas realidades. Por todo ello, Internet se ha convertido en un medio útil para quienes desean realizar conductas fraudulentas que determinan un perjuicio económico a terceros. Así, uno de los casos que ha puesto en duda el actual modelo legislativo que rige en Internet es el cierre del servicio de descargas *Megaupload*. Mientras que el FBI les acusa de delitos tales como piratería, blanqueo de capitales y evasión fiscal, muchos autores defienden un cambio en la red en el que se facilite la libertad de acceso a la información por encima de otros derechos, como son los de autor, pero que se proteja a los usuarios de la red, que en muchos casos resultan estafados por vendedores anónimos o son víctimas del *phishing*[2]. Quizás, la sentencia judicial que se dicte en los Estados Unidos respecto a Megaupload abra un nuevo camino en cuanto a la legislación de la red y el intercambio de información entre usuarios.

En este trabajo trataremos delitos tales como el blanqueo de capitales y la evasión fiscal, los cuales se han visto incrementados en los últimos años gracias a la utilización de estas nuevas tecnologías. De este modo, los delitos fiscales son unos de los delitos que más ha proliferado en la red a través de la venta de bienes y servicios online. Los hechos imponibles clásicos se basan en *una realidad en la que la conexión y presencia física son esenciales*[3]. Sin embargo, uno de los obstáculos con los que se encuentra la Administración Tributaria en Internet es, por un lado, la dificultad de identificación de las personas físicas o jurídicas que mercadean en la red utilizando seudónimos y ocultando su verdadera identificación, y, por otro lado, en el caso de ventas transnacionales, se torna complicado e, incluso a veces

2 El *phishing* es una técnica de captación ilícita de datos personales, claves para el acceso a servicios bancarios, etc., a través de correos electrónicos o páginas web que copian la apariencia de una entidad financiera. Se puede traducir al español como «pesca de datos». La técnica que suelen utilizar es muy simple. Estos delincuentes para ponerse en contacto con los usuarios utilizan las cuentas de correo electrónico enviándoles mensajes con el formato que utilizaría la entidad financiera en cuestión, pidiéndoles sus datos personales o datos bancarios con cualquier tipo de excusa para ganarse la confianza del usuario. Las excusas que suelen utilizar son de muy diversa índole: cambio de política de privacidad, posible pérdida de los datos, posible fraude en la red, etc, todo ello para conseguir sus datos sin levantar las sospechas de los usuarios. Los correos electrónicos que les envían, pidiéndoles sus datos siempre, les obligan a confirmarlos en otra página web, enlace que conducen a las «páginas web piratas» que son perfectas copias de la página web de la entidad financiera, por lo que los clientes no suelen desconfiar. De este modo, los clientes acceden a dichas páginas web piratas en las cuales el delincuente informático obtiene los datos de la persona en cuestión.

3 FERNÁNDEZ TERUELO, J.G., *Cibercrimen, los delitos cometidos a través de Internet: estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red.* Ed. Constitutio Criminalis Carolina, Oviedo, 2003, págs. 14-20.

imposible, la determinación de la jurisdicción fiscal competente, porque es imposible saber dónde se ha efectuado la transacción y dónde se encuentra la residencia fiscal de cada uno de los contratantes.

Otro de los delitos que se ha visto incrementado por el uso de la red ha sido el blanqueo de capitales. Muchos blanqueadores han aprovechado el anonimato de la red para realizar transferencias electrónicas de un lugar a otro del mundo dificultando de este modo el control y el conocimiento del verdadero origen y destino de la transacción. Los blanqueadores hacen uso de la red para llevar a cabo sus fines delictivos mediante varios métodos, como por ejemplo el Smurfing[4], mediante el cual, para no levantar sospechas sobre el origen del dinero, en primer lugar, se fracciona en cantidades más pequeñas para así evitar que superen la cantidad de 3.000 euros y eludir los controles de prevención de blanqueo de capitales (entre ellos, la obligación de declarar esas cantidades). Además, con cierta frecuencia, estos delincuentes, cuentan con la complicidad del personal de la entidad financiera, ya sean empleados o directivos, lo que les permite eludir los controles de prevención de blanqueo de capitales con mayor facilidad. Después de depositar ese dinero en varias cuentas, se efectúan transferencias a otra cuenta situada generalmente en el extranjero. Claro está, que cuantos más fraccionamientos se hagan y más entidades financieras se utilicen menor será la posibilidad de poder rastrear ese dinero. Para llevar a cabo estas operaciones los delincuentes suelen utilizar figuras tales como los «hombres de paja»[5] o la constitución de empresas pantalla para ocultar la titularidad real y el origen de los bienes utilizados. O también, las transferencias desde o hacia cuentas radicadas en paraísos fiscales donde rige plenamente el secreto bancario, etc.

El desarrollo económico y la globalización de los mercados internacionales han propiciado la aparición de nuevas formas de delito, tales como el blanqueo de capitales, que pueden contribuir a la desestabilización y lesión de los sistemas económicos. En particular, el delito de blanqueo de capitales ha adquirido suma importancia en las últimas dos décadas, lo que ha provocado por un lado, la creación de medidas preventivas del blanqueo de capitales que han ido ampliándose sucesivamente y por otro, un progresivo endurecimiento de las medidas penales.

---

4 Este procedimiento que se conoce como *smurfing/structuring*, deriva del término *smurf* con el que se denomina a unos personajes conocidos en España como «pitufos». En nuestro ámbito se denominan pitufos a aquellas personas que se encargan de fraccionar y ejecutar pequeñas operaciones económicas de enorme volumen en su conjunto, organización en la que «Papá Pitufo» es el cerebro de la operación a cuyo servicio se encuentran los pitufos. Para profundizar sobre este tipo de operaciones referidas al movimiento interno de efectivo con fraccionamiento véase PINILLA RODRÍGUEZ: «Las tipologías de blanqueo en España (I): estudio de las tipologías más frecuentes en nuestro país» en Prevención y represión del blanqueo de capitales, Estudios de Derecho Judicial, director ZARAGOZA AGUADO, Madrid, nº28, 2000, págs. 73 y ss.

5 Los hombres paja son aquellas personas con identidades falsas, indigentes o personas insolventes que se utilizan para llevar a cabo estas operaciones ocultando la verdadera identidad del titular de las operaciones.

El blanqueo de capitales es un fenómeno, tal y como lo conocemos hoy en día, relativamente reciente que nació en las legislaciones actuales vinculado al tráfico de drogas y estupefacientes. En España, con la aparición del Código Penal de 1995 se relacionaba ya con cualquier delito grave castigado con más de tres años de prisión, pero con la última reforma sufrida por el Código Penal, cualquier tipo de delito tipificado en el Código Penal español, ya puede ser el delito previo al blanqueo de capitales.

En resumen, el objetivo del blanqueo de capitales consiste en hacer que los fondos o activos obtenidos a través de actividades ilícitas aparezcan como el resultado de actividades legítimas y circulen con total apariencia de legalidad en el sistema financiero.

Al ser el blanqueo de capitales un problema transnacional, desde la Comunidad Internacional se ha tratado de impulsar la lucha contra este tipo de delincuencia, aprobándose Convenios y Tratados, los cuales han sido adaptados en la normativa interna de los Estados firmantes, adoptando medidas tanto represivas como preventivas. Los blanqueadores han aprovechado esta situación de internacionalidad para blanquear el dinero o los capitales fuera de las fronteras nacionales, lo que hace más difícil su detención, buscando para ello países donde las medidas de prevención de blanqueo de capitales sean poco o nada exigentes[6]. Así, uno de los lugares más utilizados para el blanqueo de capitales son los denominados paraísos fiscales, o territorios *offshore,* en los que se puede tanto blanquear dinero como evadir las fuertes cargas fiscales que algunas personas, tanto físicas como jurídicas, tienen en sus lugares de origen. Por eso, el intercambio de información fiscal entre los distintos Estados ha adquirido cotas impensables hace algunas décadas, todo ello en aras de la estabilidad de la economía mundial.

A pesar de todas los esfuerzos para combatir este tipo de delincuencia mediante medidas tanto preventivas como punitivas del blanqueo de capitales y los intercambios de información entre los distintos países a través de las distintas Unidades de Intercambio de Información fiscal (UIFS)[7], este tipo de delincuencia económica ha dado un paso más allá, utilizando las nuevas tecnologías para llevar a cabo sus fines delictivos. Así, han centrado sus esfuerzos en utilizar Internet como base de operaciones para blanquear las ganancias procedentes de actividades ilícitas. Es decir, las nuevas tecnologías se han convertido en una herramienta fuera del alcance de las autoridades nacionales.

---

6 ÁLVAREZ PASTOR, D. y EGUIDAZU PALACIOS, F., *Manual de prevención del blanqueo de capitales*, Marcial Pons, Madrid, 2007. pág. 22.

7 En España esta unidad se ha consolidado en el Servicio Ejecutivo Preventivo de Blanqueo de capitales, más comúnmente conocido como SEPBLAC. Este órgano es esencial en materia de prevención de blanqueo de capitales, ya que es el único que está en contacto con las entidades financieras y los sujetos obligados por la normativa preventiva, siendo el único receptor de las operaciones de *reporting sistemático*, que evalúa para después sopesar los datos, y, por ende, observar si se deriva un posible delito o infracción administrativa. El SEPBLAC analizará toda aquella información que reciba tanto de los sujetos obligados como de cualquier otra fuente, y, en el caso de que tenga indicios o certeza de blanqueo de capitales o de financiación de terrorismo, elaborará un informe de inteligencia financiera que enviará al Ministerio Fiscal o al órgano competente en ese caso.

2. MÉTODOS DE BLANQUEO DE CAPITALES

Con el aumento de las medidas preventivas del blanqueo de capitales en los últimos años, este tipo de delincuentes han tenido que desarrollar nuevas técnicas de blanqueo para poder utilizar esas grandes sumas de capital que tienen en su poder, procedentes de actividades ilícitas, con total impunidad. Por tanto, las técnicas de blanqueo de capitales son altamente sofisticadas y están dotadas de un rápido dinamismo que les permite cambiar, es decir, estar en continua adaptación para llevar a cabo las inversiones seguras del capital de origen ilícito.

Aunque cualquier tipo de actividad económica es susceptible de ser utilizada para blanquear capitales, algunos sectores son más sensibles que otros, como por ejemplo, aquellas actividades en las que se utilice habitualmente dinero en efectivo u otros instrumentos al portador como medio de pago, o aquellas en las que se ofrece un cierto grado de anonimato en las transacciones. De este modo, casas de cambio de moneda, casinos de juego, establecimientos de venta de joyas, objetos de arte y antigüedades, así como empresas dedicadas al negocio inmobiliario. Incluso se llegan a utilizar determinadas profesiones especializadas, en la mayor parte de los casos sin el conocimiento de estos profesionales, como la abogacía o los asesores fiscales que, de este modo, se han ido convirtiendo en instrumentos muy utilizados para el blanqueo de capitales[8].

Entre los distintos métodos de blanqueo de capitales nos centraremos en el uso de las nuevas tecnologías y, en especial, en el uso de las plataformas virtuales para llevar a cabo delitos tales como el blanqueo de capitales y la evasión fiscal.

3. USO DE INTERNET Y LAS NUEVAS TECNOLOGÍAS

3.1. Tarjetas anónimas y dinero electrónico

Una de las modalidades más habituales a día de hoy de blanqueo de capitales son aquellas que usan como instrumento Internet y la banca electrónica. Con las nuevas tecnologías uno de los métodos más usados por su sencillez y rapidez es el dinero electrónico[9]. Aunque los bancos *online* también exigen la identificación de sus usuarios para cumplir con la normativa preventiva del blanqueo de capitales, el elevado volumen de transferencias electrónicas y la rapidez de las transferencias hacen que el rastreo de su verdadero origen y

8 BERMEJO, M., *Prevención y Castigo del Blanqueo de Capitales. Una Aproximación desde el Análisis Económico del Derecho*, pág. 167.Tesis no publicada, leída en la Universidad Pompeu Fabra y disponible en red desde el 23/02/2010 en *http://www.tesisenred.net/handle/10803/7318?show=full*

9 El GAFI afirma que este es el método más usual de enmascaramiento utilizado por los blanqueadores, en virtud de la rapidez, distancia a la que pueden transferirse los fondos y el anonimato que permiten estas operaciones

titular sea muy difícil de llevar a cabo[10]. El GAFI considera que las transferencias electrónicas son, actualmente, uno de los principales instrumentos para blanquear capitales debido a los problemas de jurisdicción dados en los negocios sitos en Internet y por la rapidez con la que se realizan las transferencias de dinero.

También ha proliferado el uso de las tarjetas anónimas, mediante las cuales se crea un método fácil de poder repatriar los fondos desde un paraíso fiscal al país que se quiera sin tener que desvelar los datos de la cuenta *offshore* de origen. El uso de las tarjetas anónimas consiste en la interposición de un intermediario entre la cuenta *offshore* del cliente y su tarjeta de débito, la cual es totalmente independiente de la cuenta bancaria. La mayoría de programas de tarjetas anónimas funcionan con una «cuenta madre» (o *trust account*)[11], normalmente abierta por una entidad financiera y que guarda los fondos de los clientes. La entidad financiera asigna a cada cliente una subcuenta y una tarjeta con un determinado número por lo que cada vez que el cliente quiera realizar cualquier operación deberá indicar su número de tarjeta para que la cuenta madre conozca qué subcuenta es la que está operando. Una vez recibido el dinero, la financiera identificará el pago e ingresará el importe en la subcuenta correspondiente, quedando entonces el dinero disponible para su utilización o retiro por cajero automático[12].

Para evitar cualquier riesgo de blanqueo de capitales, normalmente, los bancos que tienen estas «cuentas madre» suelen cancelar las cuentas asociadas si sospechan que pueda estar produciéndose fraude o blanqueo, ya que suelen pedir algún tipo de identificación para adquirir este tipo de tarjetas anónimas (copia del pasaporte o del DNI), lo cual indica que tienen una política sólida contra el blanqueo de capitales. Sin embargo, existen instituciones financieras con una política laxa en blanqueo de capitales, o intermediarios que obtienen las tarjetas de otras empresas financieras, o que adquieren tarjetas de un solo uso, por lo que los blanqueadores de capitales suelen estar al tanto de que entidades financieras o intermediarios, sitos en estos paraísos fiscales, no cumplen con las obligaciones del *know your customer,* por lo que el riesgo de blanqueo de capitales con el uso de estas tarjeras es muy alta.

---

10 ÁLVAREZ PASTOR, D. y EGUIDAZU PALACIOS, F., *Manual de Prevención del Blanqueo de Capitales*, *op.cit.,* pág. 32.

11 Otro sistema parecido es la de las tarjetas *prepagadas* (*stored value cards*). Con este sistema, la entidad financiera en lugar de transferir el saldo a una cuenta con un número determinado, lo registra directamente en la banda magnética de la tarjeta. Las tarjetas son de un solo uso.

12 Aquí puede haber algunas variantes. Por ejemplo existen proveedores que reciben los fondos para las recargas a través de cuentas bancarias diferentes a la que alberga el programa de tarjetas (lo que lo hace aun más discreto) o permiten medios de pago alternativos como por ejemplo Cheques, *Western Union*, *Moneygram* o incluso determinadas monedas digitales. El proveedor del servicio cobrará una tarifa por recarga, generalmente un porcentaje sobre la cantidad ingresada con un importe mínimo y un pequeño cargo por cada transacción realizada.

3.2. Las nuevas tecnologías y el blanqueo de capitales: *Second life*

Como hemos podido ver en los apartados anteriores, los blanqueadores de capitales están continuamente buscando nuevas formas para poder llevar a cabo sus fines delictivos. Aunque tanto la normativa preventiva y represiva están en constante cambio para poder erradicar este fenómeno delictivo, este tipo de delincuencia parece haber encontrado en los últimos años una herramienta que les permite llevar a cabo sus delitos sin moverse de su propia casa y, sin intermediarios. Nos estamos refiriendo al uso de Internet y de las nuevas tecnologías. La doctrina ha debatido mucho acerca de los riesgos de los entornos virtuales y crece la preocupación entre algunos autores por la facilidad con que los mundos virtuales y juegos de rol online, como *Second Life* y *World of Warcraft* pueden ser utilizados para llevar a cabo delitos tales como el blanqueo de capitales o la financiación del terrorismo[13]. En la actualidad, los entornos virtuales no están sujetos a los estrictos controles financieros y los requisitos de intercambio de información del mundo real, por lo tanto, ofrecen una excelente oportunidad para los criminales para llevar a cabo sus actividades ilícitas con impunidad.

Second life (en adelante SL) es un mundo virtual creado en el año 2003 por la empresa *Linden Lab*, en el cual, para poder participar es necesario crear un avatar introduciendo una cuenta de correo electrónico y un nombre[14]. Según datos de *Linden Lab*, *SL* está formado actualmente por más de 9 millones de «residentes», los cuales pueden pasear y comprar por centros comerciales, asistir a conferencias, ir al cine, etc., donde no hay leyes ni impuestos. Este mundo virtual tiene su propia moneda, llamada dólar Linden y un producto interno bruto de 500 millones de dólares, de hecho, 750000GBP (el equivalente a unos 731.000 euros) son intercambiadas dentro de *SL* al día, pero lo más importante es que este dinero ficticio puede convertirse en dólares reales[15]. Su extensión territorial virtual tiene un total de 651 kilómetros cuadrados distribuidos en islas y continentes, donde se encuentran reproducidas virtualmente algunas de las capitales más importantes del mundo: París, Londres,

---

13 IRWIN, A., y SLAY, J., *Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft*, Originally published in the Proceedings of the 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 23rd August 2010, pág. 43. Se puede ver *online* en http://ro.ecu.edu.au/icr/5; RIJOCK, K., *China's central bank will regulate virtual currency*, 13 January 2007 en *http://www.world-check.com/articles/2007/01/13/chinas-central-bank-will-regulate-virtual-currency*; SULLIVAN, K., (2008) *Virtual money laundering and fraud: Second Life and other online sites targeted by criminals*, 3 April 2008 en *http://www.bankinfosecurity.com/articles.php?art_id=809*
TEFFT, B., *Will 5 new unregulated virtual banks become money laundering centres?* 12 January 2007 http://www.world-check.com/articles/2007/01/11/will-5-new-unregulated-virtual-banks-become-money-/

14 Un avatar es la imagen virtual de una persona real, con la diferencia de que ese segundo «yo» puede tener características físicas, psicológicas y conductuales totalmente diferentes a las que posee esa persona en el mundo real.

15 Datos extraídos del Diario digital el Economista, 3 de Septiembre de 2007. Véase en http://www.eleconomista.es.

Roma, Nueva York o Tokio. Hay sitios privados, en los cuales sólo pueden estar los avatares que hayan sido expresamente aceptados para acceder a ellas[16].

Cualquiera puede registrarse de manera gratuita introduciendo una cuenta de correo electrónico y un nombre (real o ficticio) que no se verificará por parte de Linden Lab. Sin embargo, en el momento en el que se compran los Linden dólares para poder comprar un terreno o realizar cualquier tipo de operación hay que crear una cuenta de pago (aproximadamente unos 9 dólares mensuales), con lo cual, el usuario deberá proporcionar una tarjeta de crédito o una cuenta *PayPal* con los que se estarán proporcionando datos de una persona real. Es en este punto donde se podría investigar la verdadera identidad de los delincuentes. Sin embargo, si la información que dan con esas cuentas de *Paypal* o tarjetas de crédito es ficticia, estas pequeñas comprobaciones no serán suficientes para evitar que se cometan delitos económicos dentro de este mundo virtual[17]. Muchas grandes empresas han visto la oportunidad para realizar lícitos negocios en este mundo virtual y han establecido sus sedes en *SL*. Así, por ejemplo, IBM ha adquirido quince islas, General Motors, Vodafone, Sun Microsystems, Accenture, Wells Fargo y Dell tienen sus sedes virtuales en SL.

A pesar de que existen reglas básicas para la convivencia impuestas por *Linden Lab* lo cierto es que la delincuencia organizada ha encontrado un lugar fuera del alcance de las autoridades en el que poder blanquear sin problemas las ganancias procedentes de distintos actos delictivos[18]. De hecho, la *Europol* lleva investigando varios años el funcionamiento de *SL* con la evidencia de que este mundo brinda una plataforma perfecta a los criminales para blanquear capital mediante empresas virtuales, como casinos. La escasa regulación normativa del movimiento de capitales dentro de *SL* ha impulsado movimientos de organizaciones criminales que se dedican a traspasar fondos de dólares linden por todo el planeta virtual para luego sacarlo de *SL* y convertirlos en dólares reales impunemente. Esta falta de regularización unida al enorme volumen de transferencia de dinero que se mueve por *SL* ha hecho que este mundo virtual se pueda convertir en el equivalente virtual de los sistemas *hawala*[19].

De hecho, un delincuente puede introducir el dinero procedente de cualquier actividad delictiva en *SL*, y realizar cualquier operación que desee (comprar un terreno, invertirlo en un casino o intercambiarlo con otro residente. Una vez realizada cualquiera de estas operaciones lo convertirá en dólares o euros (según la ubicación que hubiese puesto cuando creó la

16 Además, hay zonas rojas o de adultos, en las cuales el negocio del sexo representa una buena parte de las transacciones económicas que se realizan en *Second Life*.

17 Ya hemos visto en el apartado anterior, como se pueden utilizar tarjetas anónimas para operar por Internet sin desvelar la verdadera identidad del titular de la cuenta.

18 No se permite la discriminación por motivos de raza, religión u orientación sexual, el nudismo, las agresiones o desvelar datos privados de la «vida real» de otros residentes. Las normas de convivencia de *Second Life* pueden verse en *http://secondlife.com/corporate/cs.php?lang=es-ES*

19 Según SULLIVAN algunos *yihadistas* han adoptado identidades falsas en *Second Life*, para poder mover con total impunidad dinero destinado a fines terroristas en SULLIVAN, K., *Virtual Money Laundering and Fraud.* Puede verse la edición online de este artículo en *http://amltrainer.com/wp-content/uploads/KS-Virtual-Money-Laundering-and-Fraud.pdf*

cuenta, que no tiene por qué coincidir con el lugar exacto donde viva el delincuente (aunque en algunas ocasiones *Linden Lab* podrá comprobarlo). Si pone que su lugar de residencia real está en Europa, además, estas operaciones estarán gravadas con el IVA, por lo que el blanqueo de esos fondos de origen ilícito ya está realizado, ahora tienen total apariencia de legalidad[20]. La cuestión no es lo que pasa dentro de *SL,* que no deja de ser un juego de rol virtual sino que ese dinero es real y tiene consecuencias en la realidad.

Otro de los grandes problemas que ha creado el uso de las nuevas tecnologías es que a veces se torna imposible perseguir al delincuente por problemas de jurisdicción, es decir, puede tratarse de un ciudadano francés que está utilizando un equipo en Ucrania y que está negociando con un tercero situado en un tercer país y con una nacionalidad distinta[21]. En realidad *SL* es sólo un ejemplo de cómo este tipo de delincuencia económica se está adaptando a las nuevas normativas de prevención del blanqueo y de los intercambios de información entre los distintos Estados. También crean empresas falsas que hacen pagos en línea entre sí por servicios que nunca existieron, como por ejemplo trabajos de traducción que nunca fueron prestados, juegos de azar en línea, etc, etc., todo ello camuflado con facturación falsa para darle apariencia de licitud a negocios que nunca existieron.

Por todas las polémicas surgidas alrededor de este mundo virtual, *SL* ha empezado a cambiar poco a poco sus sistemas de control de intercambio de activos[22], pero no lo ha hecho para prevenir que se le relacione con este tipo de delincuencia como su principal fin, sino que en este mundo virtual también han empezado a florecer bancos virtuales que ofrecen unos altos rendimientos por depositar los ahorros en él, lo que atrajo no sólo a residentes de *SL* que tenían dinero virtual sino también a residentes que cambiaron sus bancos reales por el *Ginkofinancial*[23] para que de este modo sus ahorros tuvieran una mayor rentabilidad. Estos bancos suelen prometer altos interés, alcanzando anualmente el 20, 40, o incluso 60 por ciento[24]. Un jugador / residente puede utilizar su crédito actual o tarjeta de débito para

---

20 Según *Second Life*, se gravará con IVA las siguientes operaciones: Registro de cuenta Premium, compras en la Tienda de terrenos, cuota por uso de terreno (cuta de mantenimiento), cuota por región privada, subastas de terreno, *LindeX™ transaction fees.* Véase *http://secondlife.com/corporate/vat.php*

21 FERNÁNDEZ TERUELO, J.G., *Cibercrimen, los delitos cometidos a través de Internet: estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red.* Ed. Constitutio Criminalis Carolina, Oviedo, 2003, págs. 20-27.

22 Sobre el cambio de sistema de control de intercambio de activos puede verse en profundidad en la web de *SL: http://wiki.secondlife.com/wiki/Linden_Lab_Official:New_Policy_Regarding_Inworld_Banks*

23 Datos sobre el *Ginkofinancial* extraídos del diario El Economista, 16 de Agosto de 2007 en *http://www.economist.com/node/9661900*

24 Recordaremos un caso ya mencionado en este capítulo muy parecido en el mundo real, el caso de David Copeland y su *OSGold*. En cambio, en *Second Life*, desde el colapso financiero de *Ginko* en agosto de 2007, *Linden Lab* caso A partir del 22 de enero de 2008, se prohíbe ofrecer interés o cualquier devolución directa de la inversión (ya sea en Linden dólares u otra moneda) de cualquier objeto, como pueda ser los cajeros automáticos, situado en *Second Life*, sin certificado de registro reconocido por un gobierno o institución financiera. Según *Linden Lab*: «Vamos a aplicar esta política después de

la compra del dinero en línea y luego rescatar a los créditos por dinero real con otro jugador en otro país, y en la unidad de ese país de la moneda. Además, la cuestión que finalmente surgirá será el tema de la tributación o la falta de ella. El grupo británico *Fraud Advisory Panel* (FAP, Grupo de Consulta de Fraude en español) también ha estudiado e identificado los problemas derivados del uso de dinero en *SL* para fines de blanqueo de capitales. Así, advirtieron cómo los delincuentes o terroristas podrían transferir grandes sumas de dinero a través de las fronteras nacionales sin restricciones y con poco riesgo de ser detectados[25]. Según este grupo se deberían ampliar las normas que controlan los bancos y mercados financieros «reales» para que también controlen las transacciones financieras que se hacen dentro de *SL*. No obstante, las técnicas de blanqueo están en constante evolución por lo que este tipo de delincuencia encuentra enseguida otros métodos con los que poder darle licitud a las ganancias procedentes de sus actividades delictivas.

4. CONCLUSIONES

Como podemos observar a lo largo de las páginas de este trabajo, Internet se ha convertido en los últimos años en un medio no sólo de entretenimiento sino también en un medio usado por blanqueadores, evasores de impuestos, etc., para llevar a cabo sus fines delictivos.

En definitiva, podemos observar como poco a poco, las técnicas de blanqueo se han ido sofisticando, hasta el punto de convertirse en métodos internacionales que se amparan en el anonimato que les da la red. Es decir, que combinan diversos métodos de blanqueo de capitales, con la finalidad de agregar fases sucesivas al proceso de blanqueo, realizando transacciones de un país a otro (normalmente paraísos fiscales o territorios offshore) con la ayuda de Internet, todo ello con la finalidad de borrar el posible rastro ilícito que deje el dinero. Es decir, a mayor volumen de dinero o capitales para blanquear, mayor será el nivel de sofisticación de los métodos utilizados alcanzado, y se utilizarán las técnicas más complejas posibles y necesarias para eludir los controles estatales.

Según los datos del FMI las cifras de dinero que se blanquean significan el 5% por 100 del PIB mundial. Además, la mitad de los flujos internacionales del dinero se mueven a través de paraísos fiscales[26]. Aunque estos nuevos métodos de blanqueo de capitales que se apoyan en el uso de Internet sean difíciles de combatir por su informalidad y por el anonimato que crea, la lucha contra el blanqueo de capitales no cesa. Así, aunque la legislación en Internet aún está en fases muy iniciales, podemos poner por ejemplo, las

revisar las denuncias de los residentes, las actividades bancarias, y la ley, y lo hacemos para proteger a nuestros residentes y a la integridad de nuestra economía».

25 En el informe, *Steven Phillipsohn*, Presidente del grupo de delitos informáticos de trabajo de la FAP, declaró que «no hay nada virtual sobre la delincuencia en línea, es muy real. Es hora de que el gobierno lo tomó en serio». *http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/*

26 VVAA., Manual de Fiscalidad Internacional. IEF, edición 2007.

entidades financieras situadas en la red y en *Second life* que empiezan a aplicar las mismas políticas contra el blanqueo de capitales que el resto de los bancos con sede física. De este modo, cumplen con las medidas de diligencia debida y con el *know your customer*. Aunque en muchas ocasiones, cumplen estas medidas con cierta laxitud, con lo cual con rellenar un formulario para abrir una cuenta ya es suficiente[27]. Incluso, a pesar de estas medidas preventivas, se sigue permitiendo el uso de los *nominees* (directores fiduciarios) que ayudan a ocultar la identidad de los propietarios reales de las empresas. Tales medidas, junto con la normativa preventiva, servirán, sin duda, para prevenir la expansión internacional del blanqueo de capitales.

5. BIBLIOGRAFÍA

Álvarez Pastor, D. y Eguidazu Palacios, F., *Manual de prevención del blanqueo de capitales*, Marcial Pons, Madrid, 2007

Bermejo, M., *Prevención y Castigo del Blanqueo de Capitales. Una Aproximación desde el Análisis Económico del Derecho*, pág. 167.Tesis no publicada, leída en la Universidad Pompeu Fabra y disponible en red desde el 23/02/2010 en *http://www.tesisenred.net/handle/10803/7318?show=full*

Fernández Teruelo, J.G., *Cibercrimen, los delitos cometidos a través de Internet: estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red.* Ed. Constitutio Criminalis Carolina, Oviedo, 2003.

Irwin, A., y Slay, J., *Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft*, Originally published in the Proceedings of the 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 23rd August 2010, pág. 43. Se puede ver *online* en http://ro.ecu.edu.au/icr/5; Rijock, K., *China's central bank will regulate virtual currency*, 13 January 2007. Retrieved March, 9th, 2012 from *http://www.world-check.com/articles/2007/01/13/chinas-central-bank-will-regulate-virtual-currency*;

Pinilla Rodríguez: «Las tipologías de blanqueo en España (I): estudio de las tipologías más frecuentes en nuestro país» en *Prevención y represión del blanqueo de capitales, Estudios de Derecho Judicial*, director Zaragoza Aguado, Madrid, nº28, 2000.

Sullivan, K., (2008) *Virtual money laundering and fraud: Second Life and other online sites targeted by criminals*, 3 April 2008. Retrieved March, 9th, 2012 from en *http://www.bankinfosecurity.com/articles.php?art_id=809.*

27 Aunque en el caso de que se depositen cantidades importantes es frecuente que el banco solicite documentación adicional que pruebe el origen del dinero, aunque estas informaciones siempre serán privadas y protegidas por el riguroso secreto bancario de estos territorios.

Tefft, B., *Will 5 new unregulated virtual banks become money laundering centres?* 12 January 2007. Retrieved March, 9th, 2012 from http://www.world-check.com/articles/2007/01/11/will-5-new-unregulated-virtual-banks -become-money-/

CAMBIAR LAS REGLAS DEL (VIDEO)JUEGO. MECANISMOS DE CONTROL CONTRACTUAL EN PLATAFORMAS DE ENTRETENIMIENTO ONLINE

Antoni Rubí Puig
Profesor Lector de Derecho Civil de la Universitat Pompeu Fabra

RESUMEN: El objeto de este artículo es examinar el alcance jurídico de las facultades de exclusión y control que otorgan los derechos de propiedad intelectual y, sobre todo, el derecho de contratos a quienes ponen a disposición online un videojuego u otro producto de entretenimiento. A partir de una sentencia norteamericana reciente, *MDY Industries v. Blizzard Entertainment*, se relacionan las cuestiones que puede plantear el recurso a los remedios propios del derecho de contratos, frente a las soluciones jurídicas previstas para la infracción de derechos de autor, en el control de conductas de usuarios de una plataforma online, como, por ejemplo, en el supuesto de hecho enjuiciado, la prohibición establecida en una licencia de software de utilizar programas robot en interacción con un videojuego.

A partir de la discusión del caso citado, el artículo identifica los principales problemas que genera la interrelación entre derechos de autor y derecho de contratos y sus efectos sobre la innovación y la competencia en el mercado. El entendimiento de dicha interrelación debe centrarse, entre otros aspectos, en examinar: (1) la cuestión acerca de si, gracias a la autonomía privada, mediante una licencia de usuario, unas condiciones de uso predispuestas o, en su caso, un contrato negociado entre las partes se puede alterar el equilibrio de intereses diseñado por el legislador en la regulación sobre derechos de autor; (2) la formación del consentimiento en el caso de licencias de usuario u otros contratos; (3) los límites al principio de eficacia relativa del contrato y a la creación de facto de derechos con eficacia absoluta; (4) las diferencias en el régimen de remedios disponibles ante un incumplimiento de una licencia que proporcionan en derecho español, por un lado, el TRLPI y, por otro, el Código Civil; y (5) los límites que puede imponer el derecho de defensa de la competencia al uso del derecho de contratos.

PALABRAS CLAVE: videojuegos, derechos de autor, licencias de usuario, incumplimiento contractual, remedios, medidas tecnológicas de protección.

1. INTRODUCCIÓN

Durante siglos ha sido habitual que quienes participaban en actividades lúdicas o deportivas modificaran sus reglas para adaptarlas a las preferencias propias. Los cambios en las reglas más o menos formalizadas de un juego, ya sean espontáneos o premeditados, muestran un escenario de innovación descentralizada, que históricamente ha contribuido a la aparición de nuevas modalidades deportivas y de nuevas variedades de un mismo juego[1].

1 El concepto de innovación descentralizada y los impedimentos que conllevan las regulaciones sobre propiedad intelectual cuentan con una nutrida literatura. Véanse, entre otros, Von Hippel, E. (2005).

Este panorama es mucho más limitado o casi nulo en el entretenimiento online y, en particular en los videojuegos en línea, en los cuales la tecnología y el derecho pueden prácticamente eliminar la posibilidad de alterar las reglas de un determinado juego. Las facultades de exclusión que otorgan los derechos de propiedad intelectual y, sobre todo, el derecho de contratos permiten a quien pone a disposición online un videojuego u otro producto de entretenimiento ejercer un amplio poder de control sobre lo que sus usuarios hacen con él y, en particular, pueden poner palos a las ruedas de la innovación, ya en el contenido de las reglas del juego, ya en la creación y desarrollo de productos y servicios complementarios.

El objeto de este artículo es examinar el alcance jurídico de dichas facultades de control y analizar las ventajas comparativas respectivas de los remedios por incumplimiento contractual y de los instrumentos propios del derecho de autor. Para ello, se analiza una sentencia norteamericana reciente, *MDY Industries v. Blizzard Entertainment*[2], dictada el pasado 14 de diciembre de 2010 por el Tribunal de Apelaciones del Noveno Circuito, según el cual, en el caso de un popular videojuego online (*World of Warcraft*), las soluciones jurídicas frente a la infracción de derechos de autor cobran un papel residual frente al derecho de contratos para controlar las conductas de los usuarios de la plataforma, como, por ejemplo, en el supuesto de hecho enjuiciado, el desarrollo de un programa robot que permitía jugar automáticamente los primeros niveles del juego.

A partir de la discusión del caso citado, el artículo ofrece un marco general para examinar la interrelación entre derechos de autor y derecho de contratos en el control de productos de entretenimiento online y sus efectos sobre la innovación y la competencia en el mercado.

2. EL ASUNTO *MDY INDUSTRIES V. BLIZZARD ENTERTAINMENT*

2.1. Hechos

Blizzard Entertainment, Inc. (en adelante, Blizzard) es una productora titular residual de los derechos de propiedad intelectual sobre *World of Warcraft* (WoW), un popular videojuego online multijugador cuyos usuarios, bajo la apariencia de personajes (avatares) como elfos, gnomos, orcos o enanos, superan pruebas e interactúan en los territorios virtuales de Azeroth.

El objetivo del juego consiste en completar los diferentes niveles de la plataforma en cuyo curso sus usuarios, cooperando con otros jugadores de su misma facción, la Alianza o la Horda, combaten monstruos, superan retos y pruebas y recogen algunos premios, como nuevas armas, protecciones y armaduras o el dinero corriente en la plataforma virtual. WoW también ofrece a sus usuarios la posibilidad de conversar con otros jugadores de su facción mediante un sistema de chat para así organizarse conjuntamente y maximizar los resultados esperados de su cooperación.

Democratizing Innovation. Cambridge: MIT Press; y Shirky, C. (2010). *Cognitive Surplus: How Technology Makes Consumers Into Collaborators*. New York: Penguin.

2 *MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928 (9th Cir. 2010).

Desde la creación del videojuego WoW en noviembre de 2004, ha atraído a más de diez millones de usuarios, una cuarta parte de los cuales en Estados Unidos y, en la actualidad, es el videojuego de rol multijugador (*massively multiplayer online role-playing game* (MMORPG)) más popular del mundo.

El uso del videojuego requiere, en general, además de la instalación de una copia en el hardware del jugador, del pago de cuotas mensuales de suscripción. Blizzard también ofrece la posibilidad de jugar gratuitamente, aunque las opciones de juego son mucho más limitadas.

Michael Donnelly, un usuario de WoW y programador, desarrolló en marzo de 2005 un programa robot («bot») al que denominó «Glider», que permitía automatizar el juego en los primeros niveles sin necesidad de que el jugador estuviera ante su pantalla. Durante su funcionamiento, el programa Glider no modificaba, ni reproducía el código del software de cliente de WoW, y no evitaba el pago de la suscripción mensual de los usuarios a Blizzard. El programa carecía de cualquier valor comercial o funcional al margen de WoW. En un primer momento, Glider no fue diseñado para evitar que fuera detectado por Blizzard. En verano de 2005, tras asegurarse de que la licencia de usuario del programa (EULA) y las condiciones generales de uso (TOU) de WoW no prohibían el uso de robots, la sociedad de Donnelly, MDY Industries, LLC, empezó a comercializar Glider al precio de 15 a 25 dólares por copia.

Ante quejas recibidas por usuarios, Blizzard implementó, en septiembre de 2005, un programa denominado «Warden» que impedía a los jugadores que utilizaran programas o aplicaciones de terceros –entre ellos, el bot Glider– conectarse a los servidores de Blizzard y en efecto, disfrutar del videojuego.

Entonces, MDY modificó el programa Glider para evitar que fuera detectado por Warden y desarrolló, además, una nueva versión denominada «Glider Elite», que, a cambio de una suscripción mensual de 5 dólares, ofrecía protección adicional frente a los programas de detección implementados por Blizzard. A finales de 2005, MDY informó a través de su website que la utilización de Glider por parte de un jugador infringía los términos de uso del programa predispuestos por Blizzard.

La aventura comercial de MDY fue, en un principio, un éxito. Los beneficios de la empresa, a septiembre de 2008, habían alcanzado los 3.5 millones de dólares, tras vender más de 120.000 copias de Glider.

2.2. El conflicto entre las partes

Según Blizzard, la utilización de Glider le ocasionó diferentes daños y perjuicios consistentes en los gastos de responder a más de 400.000 reclamaciones de usuarios relacionadas con bots (unos 94.000 dólares anuales); y en las pérdidas de suscripciones mensuales, pues los usuarios de Glider llegaban más pronto a la final del videojuego. Asimismo, Blizzard, como titular de los derechos de autor sobre el videojuego, ha alegado en repetidas ocasiones que debe poder ejercer un control máximo de las experiencias que pueden obtener los

usuarios del producto, así como de todos los productos y servicios que puedan desarrollarse a partir del videojuego[3].

Por ello, envió en agosto de 2006 un requerimiento a MDY para que cesara en la utilización de imágenes del videojuego en su sitio web y en la comercialización de Glider. MDY retiró las capturas de pantalla de su sitio web pero solicitó que se le clarificara la petición formulada en relación con Glider. Poco después, Blizzard amenazó a MDY con emprender acciones judiciales.

MDY y Donnelly se adelantaron a Blizzard e iniciaron ellos mismos un procedimiento declarativo y solicitaron al juez una declaración según la cual el programa Glider no habría infringido ni los derechos de autor de Blizzard, ni otros derechos e intereses de ésta.

Blizzard contestó a la demanda y, además, reconvino y ejercitó acciones de cesación e indemnizatorias fundadas en las conductas siguientes:

(a) Infracción contributiva de derechos de autor (*contributory copyright infringement*) e infracción vicaria de derechos de autor (*vicarious copyright infringement*).

(b) Elusión de medidas técnicas de protección (pretensiones derivadas de la *Digital Millenium Copyright Act* (DMCA)[4], §§ 1021(a)(2) y (b)(1)).

(c) Inducción a la infracción contractual (*tortious interference with contract*, con arreglo al derecho de contratos de Arizona).

La historia procesal del caso es compleja. A lo que aquí interesa, el tribunal de distrito de Arizona resolvió en *summary judgment* que las ventas de Glider infringían contributivamente y vicariamente los derechos de autor de Blizzard y que suponían una interferencia negligente en los contratos que unían a Blizzard con sus clientes. Después del *bench trial*, resolvió el Tribunal que MDY había infringido, además, los §§ 1021(a)(2) y (b)(1)) DMCA, y, en consecuencia, ordenó el cese en la comercialización de Glider y condenó a MDY y a Donnelly a satisfacer una indemnización de 6.5 millones de dólares[5].

2.3. La sentencia dictada en apelación

MDY y Donnelly recurrieron la decisión ante el Tribunal de Apelaciones para el Noveno Circuito, que dictó sentencia el 14 de diciembre de 2010 con ponencia de la Juez Con-

---

3 Esto es, recurriendo a la distinción realizada por Mark Lemley, Blizzard acude a una justificación *ex post* de los derechos de propiedad intelectual, según la cual el ordenamiento atribuye a un creador no únicamente los incentivos suficientes para que una obra se desarrolle en primer lugar sino unas facultades máximas que permitirían ejercer un control y una apropiación de las externalidades positivas generadas con aquélla. Lemley, M. (2004). Ex Ante versus Ex Post Justifications for Intellectual. Property. *University of Chicago Law Review* 71, 129. Se trata de una concepción demsetziana de los derechos de propiedad intelectual criticada por el propio Lemley. Véanse Frischmann, B. y Lemley, M. (2007). Spillovers. *Columbia Law Review* 107, 257; y Frischmann, B. (2007). Evaluating the Demsetzian Trend in Copyright Law. *Review of Law and Economics* 3, 649.

4 *Digital Millenium Copyright Act* (DMCA), 17 U.S.C. §§ 512, 1201–1205, 1301–1332; 28 U.S.C. § 4001.

5 *MDY Industries, LLC v. Blizzard Entertainment, Inc. et al.,* 616 F. Supp. 2d 958 *(*D. Ariz. 2009*).*

suelo Callahan. El Tribunal anuló las condenas a los recurrentes derivadas de la infracción de derechos de autor y del artículo 1021(b)(1) DMCA y resolvió que quedaban pendientes de análisis cuestiones de hecho relativas al *tort* de inducción a la infracción contractual, por lo que era necesaria su discusión ante un jurado. Se analizan a continuación los diferentes pronunciamientos de la sentencia.

2.3.1. Responsabilidad ajena por infracción de derechos de autor (Secondary Infringement)

En la jurisprudencia norteamericana sobre propiedad intelectual se han desarrollado varias doctrinas sobre la responsabilidad civil por infracciones de derechos de autor cometidos por un tercero. Estas categorías se enmarcan dentro de la etiqueta general de «infracción secundaria»[6].

Para acreditar una infracción secundaria, es necesario primero probar una infracción directa de derechos de autor por un tercero. Así, en el asunto en cuestión, Blizzard debería probar que es titular de derechos de autor sobre la obra pretendidamente infringida y que los usuarios de Glider han vulnerado alguno de sus derechos de exclusiva reconocidos por la legislación federal[7]. Entonces, MDY podría resultar responsable contributiva por vulneración de derechos de autor (*contributory infringement*) si hubiera inducido o animado intencionalmente la infracción directa por parte de los usuarios de Glider[8]. O, por otra parte, podría resultar responsable vicaria (*vicarious infringement*) si MDY hubiera podido controlar efectivamente la actividad supuestamente infractora de los usuarios de Glider y obtener un beneficio económico directo de dicha actividad.

Para analizar la posible infracción directa de derechos de autor por los usuarios de Glider, resulta necesario examinar el funcionamiento de los diferentes programas que componen el videojuego.

El software de WoW cuenta con dos elementos:

a) El software de cliente que el usuario instala en su ordenador. Tradicionalmente los usuarios adquirían una copia física del programa, por ejemplo en un CD en un establecimiento mercantil, que se acompañaba de una licencia final de usuario o EULA. En la actualidad, también es posible la adquisición de una copia online. En cualquier caso, el cliente debe aceptar el EULA en dos ocasiones: antes de instalar el programa en su ordenador y la primera vez que carga el programa.

b) El software de servidor al que el usuario accede online mediante su suscripción. El jugador debe aceptar las condiciones de uso del sitio web del juego (TOU), también en dos ocasiones: cuando se crea una cuenta de usuario y la primera vez que se produce una conexión al servicio online. Las condiciones generales de uso son muy claras en la

6 Véase Lichtman, D. y Landes, W. (2003). Indirect Liability for Copyright Infringement: An Economic Perspective. *Harvard Journal of Law & Technology* 16, 395.

7 Copyright Act, 17 U.S.C. §§ 101-1332 (2012).

8 Véase *MGM Sutdios Inc. v. Grokster, Ltd*, 545 U.S. 913 (2005).

prohibición de la utilización de bots. El apartado 4 (B) TOU establece: *«You agree that you will not... (ii) create or use cheats, bots, «mods», and/or hacks, or any other third-party software designed to modify the World of Warcraft experience; or (iii) use any third-party software that intercepts, «mines», or otherwise collects information from or through the Program or Service».*

Cuando se juega a WoW, se producen copias temporales de los programas informáticos que componen el software de WoW en la memoria RAM (*Random-Access Memory*) de los equipos de los usuarios, tanto si usan Glider o no. Dichas copias temporales constituyen un acto de reproducción protegido mediante derechos de autor[9]. En efecto, son susceptibles de constituir una infracción del derecho de reproducción excepto si: a) el usuario es el propietario legítimo de una copia del software (*essential step defense*); o b) es un licenciatario legítimo que utiliza el software de acuerdo con su licencia o condiciones de uso.

En primer lugar, para el tribunal, si los clientes de WoW son propietarios de una copia del software, los usuarios de Glider no infringirían el derecho de reproducción al realizar las citadas copias RAM en sus ordenadores y, en efecto, MDY no sería responsable por infracción secundaria de derechos de autor. Para ello, debe tenerse en cuenta la *essential step defense* (17 U.S.C. 117 (a)(1)[10]), esto es, el derecho a realizar actos de reproducción necesarios para la utilización del programa de ordenador[11].

Para evitar la aplicación de esta defensa y, sobre todo, para evitar el agotamiento del derecho de distribución en aplicación de la *First Sale Doctrine*[12], los productores de software han recurrido a caracterizar la comercialización de sus productos como actos no transmisivos de la propiedad sobre las copias del software[13]. Para ello y, a pesar de los problemas dogmáticos que implica, se dice que el software únicamente se licencia, pero no se transmite. Se trata de una práctica consolidada en el sector, cuyos orígenes se remontan a un momento histórico de incertidumbre sobre las posibilidades de acudir al ordenamiento jurídico para proteger las inversiones y esfuerzos desplegados en el desarrollo de software y, en particular, acerca de cuáles deberían ser los instrumentos más adecuados para articular tal protección

9 Véase Perzanowski A (2010). Fixing RAM Copies, *Northwestern University Law Review* 104, 1067.

10 «117(a) Making of Additional Copy or Adaptation by Owner of Copy. — Notwithstanding the provisions of section 106, it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided: (1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, […]».

11 Véase, en la legislación española, el artículo 100.1 TRLPI.

12 La doctrina está codificada en 17 U.S.C. §§ 109. El antecedente clásico es una sentencia ya centenaria del Tribunal Supremo federal: *Bobbs-Merrill Co. v. Straus*, 210 U.S. 339 (1908).

13 Véanse Determann L. y Fellmeth, A. (2001). Don't Judge a Sale by Its License: Software Transfers Under the First Sale Doctrine in the United States and the European Community. *University of San Francisco Law Review* 36, 1; y Carver, B. (2010). Why License Agreements Do Not Control Copy Ownership: First Sales and Essential Copies. *Berkeley Technology Law Journal* 25, 1887.

(secretos empresariales, contratos, acciones por competencia desleal, derechos de patente, derechos de autor u otros *derechos sui generis*)[14].

El Tribunal recurrió a *Vernor v. Autodesk*[15], un asunto reciente en la discusión sobre la distinción entre licencia y venta en la comercialización de software, para afirmar, como regla general, que el usuario de un programa de ordenador es un licenciatario y no el propietario de una de las copias del mismo en aquellos supuestos en los cuales el titular de los derechos de autor hubiera (i) especificado que el usuario fuere un licenciatario; (ii) restringido significativamente las posibilidades de transmisión del programa; y (iii) impuesto restricciones notables al uso del programa. Aplicando estas consideraciones a la licencia de Blizzard, el Tribunal resolvió que los usuarios de WoW son meros licenciatarios del programa en cuestión:

i) Blizzard se reservaba la titularidad del software y ofrecía una licencia limitada y no exclusiva.

ii) Restringía la alienación de la copia del programa al condicionar la transmisión a la entrega de toda la documentación y del paquete original y a la aceptación del EULA por el adquirente ulterior y obligaba a borrar cualquier copia en el ordenador del usuario.

iii) Solo se permitían usos no comerciales del programa; no se permitía jugar en cyber-cafes u otros sitios públicos sin autorización previa de Blizzard, y podía cancelarse la cuenta de un usuario. Blizzard puede alterar, además y en cualquier momento, las características del juego remotamente.

Puesto que los usuarios de WoW no ostentan el dominio sobre las copias del software, no están protegidos por la *essential step defense* para la reproducción de copias RAM y, en efecto, su actuación infringiría el derecho de exclusiva de Blizzard salvo que estén amparados por la licencia.

En segundo lugar, el Tribunal examinó esta última cuestión, esto es, si el usuario del videojuego y, en particular, quien utilizare Glider, era un licenciatario legítimo que empleaba el software de acuerdo con su licencia o condiciones de uso predispuestas por Blizzard.

Como hemos señalado, la licencia era muy clara en la prohibición de la utilización de bots. En efecto, los usuarios que utilizaban conjuntamente WoW y Glider no llevaban a cabo un uso del programa de Blizzard de acuerdo con la licencia predispuesta y, en consecuencia, no habría, de entrada, una autorización para realizar la reproducción. Mas, para que se produzca una infracción del derecho de reproducción u otros derechos exclusivos de explotación, resulta necesario que la cláusula infringida en el contrato o licencia consista en una condición (*condition*) de uso del derecho de propiedad intelectual y no de otro pacto contractual independiente (*covenant*). En caso de duda sobre la interpretación de la licencia, debe presumirse que la cláusula en cuestión constituye un pacto contractual y no una condición.

---

14 Véase Madison, M. (2003). Reconstructing the Software License. *Loyola University Chicago Law Journal* 35, 275.

15 *Vernor v. Autodesk, Inc.*, 621 F.3d 1102 (9th Cir. 2010). Cfr. con *UMG Recordings, Inc. v. Augusto*, 628 F.3d 1175 (9th Cir. 2011).

El Tribunal resuelve que la referida cláusula es una obligación, por lo que su contravención sólo puede dar lugar a un incumplimiento contractual, pero no a una infracción de derechos de autor. El Tribunal examina diversas restricciones en la licencia y distingue entre algunas que constituirían condiciones en el uso de los actos comprendidos por los derechos exclusivos de propiedad intelectual y otras obligaciones contractuales desvinculadas del ámbito objetivo de los derechos de autor.

Para el Tribunal, para que pueda existir infracción de derechos de autor fundada en el incumplimiento de una licencia de usuario, deben darse dos requisitos cumulativos: i) el acto supuestamente infractor –por ejemplo, una copia provisional ilegítima– debe exceder los límites de la licencia o las conductas autorizadas por el titular; y ii) debe estar relacionada con un derecho de autor exclusivo reconocido legalmente.

Para el tribunal debe existir un vínculo entre la condición y los derechos de autor exclusivos del licenciante[16]. La única excepción, para el tribunal, es la obligación de pago: si se usa el software sin pagar el precio o contraprestación pactado con el titular, puede existir infracción de derechos de autor además de incumplimiento contractual.

Para el tribunal, «si resolviéramos en otro sentido, Blizzard –u otro titular de derechos de autor sobre un programa informático– podría designar cualquier tipo de conducta que no gustara durante el uso del programa como una infracción de derechos de autor, al condicionar la licencia a la abstención por parte del usuario de incurrir en aquélla». Se produciría una autoatribución de derechos más allá de los proporcionados por la legislación.

La distinción es muy relevante, por cuanto la protección que ofrece el derecho de contratos es, de entrada, mucho más limitada que la proporcionada por el derecho de propiedad intelectual. Las diferencias esenciales se resumen en las que siguen:

a) Los remedios por incumplimiento contractual son más restringidos (interés contractual positivo), mientras que, en el ámbito de los derechos de autor, además de los daños producidos, existen posibilidades de expropiar los beneficios del infractor. Otra diferencia importante radica en la posibilidad de ejercitar acciones de cesación en materia de propiedad intelectual. Asimismo, la legislación norteamericana permite, en algunos supuestos, la compensación de daños fijados legalmente de un máximo de 150.000 dólares por acto de infracción y obra, y el comiso de los instrumentos y copias infractores. Finalmente, el régimen de las costas procesales en el ámbito de los derechos de autor es diferente del régimen general del derecho procesal civil y permite acudir a criterios de vencimiento objetivo en caso de prevalecer en el pleito.

b) Principio de eficacia relativa del contrato. Los remedios propios del incumplimiento contractual se predican de las partes en una relación obligatoria, pero no alcanzan a terceros ajenos al contrato. En cambio, los derechos de autor y, en general, los derechos de propiedad tienen una eficacia *erga omnes* por lo que los remedios jurídicos previstos para su infracción o perturbación pueden ejercerse frente a sujetos no necesariamente

16 Van Houweling, M. (2011). Touching and Concerning Intellectual Property. *Santa Clara Law Review* 51, 1063.

ligados por un contrato. Así, en el caso de que el primer usuario legítimo transmita su copia de una obra a un tercero (*downstream users*) y se entienda que no hay subrogación contractual, el titular de derechos de autor quedaría desprotegido si las conductas contractuales incumplidas se configuraran como pactos y no condiciones para la realización de actos de explotación de derechos de autor. Dicha limitación supone, además, una dificultad añadida a la realización de estrategias de discriminación de precios en el ámbito de la explotación de obras protegidas por derechos de autor[17].

c) Imposibilidad de acudir a las doctrinas de la infracción contributiva o vicaria de derechos de autor. El afectado deberá acudir a otras vías mucho más limitadas como los *business torts* o, en su caso, acciones por competencia desleal, cuyo régimen es estatal y, en efecto, puede resultar más costosa su aplicación unitaria en el mercado norteamericano.

En definitiva, un usuario de WoW que utilice Glider u otro bot para jugar automáticamente al videojuego incumple la licencia y contraviene sus deberes contractuales, pero no infringe los derechos de autor de Blizzard. En consecuencia, al no haber una infracción directa de derechos de autor por parte de los usuarios de Glider, no puede atribuirse responsabilidad a MDY por infracción secundaria de derechos de propiedad intelectual.

2.3.2. Pretensiones derivadas de la Digital Millenium Copyright Act: elusión de medidas tecnológicas de protección

Blizzard desarrolló una medida tecnológica para controlar el uso de robots en el marco del videojuego WoW, que denominó «Warden». Warden cuenta con dos componentes diferentes:

a) Un módulo denominado «scan.dll», que examina la copia RAM del usuario antes de permitir la conexión a los servidores de WoW. Si scan.dll detecta un bot, como por ejemplo Glider, no permite al usuario conectarse a los servidores y jugar. MDY modificó Glider para eludir scan.dll de forma que Glider no se cargara hasta despúes de que scan.dll hubiera hecho la comprobación de la copia RAM.

b) Un módulo residente que funciona periódicamente mientras un usuario está conectado a los servidores de WoW. El componente solicita al ordenador del usuario el envío de informes sobre el código copiado en la memoria RAM para detectar pautas de utilización de bots. En caso de detección, el módulo desconecta al usuario de los servidores.

Según Blizzard, el programa robot Glider infringía normas sobre elusión de dichas medidas tecnológicas. En particular, la discusión se centró en determinar MDY vulneraba las siguientes normas de la DMCA:

17 Véase Hovenkamp, H. (2010). Post-Sale Restraints and Competitive Harm: The First Sale Doctrine in Perspective. *NYU Annual Survey of American Law* 2010, 101. En contra, Katz, A. (2011). What Antitrust Law Can (and Cannot) Teach About the First Sale Doctrine. Disponible en http://ssrn.com/abstract=1845842 (consultado en 24.3.2012).

a) 17 U.S.C. § 1201(a)(2), que prohíbe fabricar, importar, ofrecer al público, proporcionar o poner en el tráfico de algún otro medio tecnologías, productos, dispositivos o servicios que sirvan para eludir medidas tecnológicas implementadas para *controlar efectivamente el acceso* a una obra protegida mediante derechos de autor[18].

b) 17 U.S.C. § 1201(b)(1), que prohíbe fabricar, importar, ofrecer al público, proporcionar o poner en el tráfico de algún otro medio tecnologías, productos, dispositivos o servicios que sirvan para eludir medidas tecnológicas implementadas para *proteger efectivamente* un derecho de autor[19].

Para examinar la posible vulneración de dichas normas, las partes y los tribunales que conocieron del caso diseccionaron el videojuego en tres elementos diferentes, protegibles por derechos de autor de forma independiente:

a) Elementos literales del videojuego: consisten en la expresión original contenida en el código fuente que, al realizar las copias permanentes o temporales del programa, se almacena en los ordenadores de los usuarios.

b) Elementos no literales individuales: consisten en los más de 400.000 componentes visuales y audibles del videojuego, por ejemplo, la imagen de un monstruo o sus rugidos.

c) Elementos no literales dinámicos: consisten en la obra que se crea a partir de la experiencia en tiempo real que supone el juego y que conlleva la movilidad en el espacio virtual de Azeroth y encontrarse pruebas, retos, monstruos u otros jugadores.

Para el tribunal de distrito, no se producía una infracción del artículo 1201(a)(2) en relación con los elementos literales: Warden no afectaba el acceso al código fuente del programa que se instala en el ordenador del usuario sin necesidad de conexión a los servidores de WoW. Asimismo, también resolvió que no se vulneraba la norma en relación con los elementos no literales individuales, por cuanto se contenían en el código instalado en el

18 17 U.S.C. § 1201(a)(2): «No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that— (A)is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title; (B)has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or (C)is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title». Véase, en España, artículo 160 TRLPI.

19 17 U.S.C. § 1201(b)(1): «(1)No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that— (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; (B)has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or (C)is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof». Véase, en España, artículo 160 TRLPI.

ordenador de usuario y Warden no controlaba en ningún caso el acceso a los mismos. En cambio, resolvió que existía una infracción de los artículos 1201 (a)(2) y de 1201(1)(b) en relación con los elementos no literales dinámicos. Para el tribunal de distrito, sólo se podía acceder a tales elementos mediante la conexión a los servidores de WoW y Glider permitía suprimir los efectos de Warden para acceder a los mismos.

El Tribunal de Apelación confirma el fallo del Tribunal de distrito en relación con el artículo 1201(a)(2), pero no respecto del artículo 1201(1)(b). Esto es, resolvió que la tecnología Warden se dirigía a controlar el acceso a obras protegidas por derechos de autor –únicamente los elementos no literales dinámicos– pero no se dirigía a proteger efectivamente tales derechos.

Para ello, el Tribunal de Apelaciones recurrió a una interpretación novedosa de la regulación sobre medidas tecnológicas de protección, que se apartaba de los precedentes judiciales en la materia[20] y que ha sido muy criticada[21]. Con arreglo al tribunal, para que se produzca una infracción del artículo 1201(a)(2) no resulta necesario que la medida tecnológica de protección implementada tenga por objeto evitar eventuales infracciones de derechos de autor. Para el Tribunal, examinando los antecedentes legislativos de la norma, se trata de una pretensión diferente, independiente de la existencia o no de infracción de derechos de autor. En otros términos, el Tribunal crea «de facto» un derecho de acceso a obras protegidas que no había existido nunca en el copyright norteamericano que protege frente, al menos, algunas formas de *digital trespass*.

2.3.3. Inducción a la infracción contractual

Según el Tribunal, los elementos que debería acreditar Blizzard, con arreglo al derecho de Arizona, para que prosperara la acción basada en la inducción a la infracción contractual son los que siguen: a) la existencia de una relación contractual válida; b) el conocimiento por parte de MDY de dicha relación; c) la interferencia intencional de MDY que induzca o genere un incumplimiento de los deberes contractuales; d) la ilicitud de dicha interferencia; y e) la causación de daños.

Para el tribunal, concurrían cuatro de los cinco elementos en el comportamiento de MDY. Mas, existirían dudas de hecho sobre el carácter ilícito de la interferencia. Para despejar dicha incertidumbre, el derecho de Arizona recurre al test propio del *Restatement (Second) of Torts* § 767, que contiene, a su vez, siete elementos: 1. La naturaleza de la conducta del sujeto; 2. Las finalidades perseguidas por éste; 3. Los intereses de la otra parte en los que aquél interfiere; 4. Los intereses perseguidos por esta otra parte; 5. Los intereses sociales en proteger la libertad de acción de quien interfiere y los intereses de la otra parte; 6. El carácter

20 *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178 (Fed. Cir. 2004).

21 Véanse, por ejemplo, Shikowitz, R. (2010). Note, License to Kill: *MDY v. Blizzard* and the Battle over Copyright in World of Warcraft. *Brooklyn Law Review* 75, 1015; y Barnes, P. (2011). The Prospects for Protecting News Content Under the Digital Millennium Copyright Act. *Harvard Journal of Sports & Entertainment Law* 3, 201.

próximo o remoto de la conducta del primero en relación con la interferencia; 7. Las relaciones entre las partes[22].

Aplicando dicho test, según el Tribunal, faltaría acreditar determinadas cuestiones de hecho que obligarían a seguir el procedimiento en relación con los cinco primeros puntos. En consecuencia, el Tribunal estimó la pretensión de MDY para que tales cuestiones de hecho se dilucidaren ante un jurado.

El tribunal señaló, en cualquier caso, que una acción por inducción a la infracción contractual no quedaba desplazada por la legislación federal sobre derechos de autor que impide acudir a remedios o pretensiones jurídicos que puedan resultan equivalentes a los derechos de autor previstos legalmente (*copyright preemption*[23]). Citando *Altera Corp. v. Clear Logic, Inc.*[24], recordó de nuevo que estamos ante un pacto contractual incluido en las condiciones de uso y no ante una condición relativa a la realización de actos comprendidos en el ámbito objetivo de los derechos exclusivos de autor.

3. PROTAGONISMO DEL DERECHO DE CONTRATOS

El Tribunal en *MDY v. Blizzard* centró su decisión en torno a fundamentos no ceñidos expresamente a la infracción de derechos de autor. Los remedios previstos por el derecho de propiedad intelectual quedan relegados a un segundo plano y, en cambio, cobran protagonismo los remedios propios del derecho de contratos y la tecnología, auxiliada por la normativa sobre elusión de medidas tecnológicas de protección.

De entrada, el derecho de contratos permite al titular de los derechos de explotación sobre una obra –por ejemplo, un videojuego online– escoger el modelo de puesta a disposición de sus productos en el mercado, así como las circunstancias en que ésta tendrá lugar, en particular, el precio y las limitaciones al uso que el mercado le permita. Con ello, quien se encarga de la explotación comercial de una obra protegida por derechos de autor puede

22 *Restatement (Second) of Torts* § 767: «In determining whether an actor's conduct in intentionally interfering with a contract or a prospective contractual relation of another is improper or not, consideration is given to the following factors: (a) the nature of the actor's conduct, (b) the actor's motive, (c) the interests of the other with which the actor's conduct interferes, (d) the interests sought to be advanced by the actor, (e) the social interest in protecting the freedom of action of the actor and the contractual interests of the other, (f) the proximity or remoteness of the actor's conduct to the interference and (g) the relations between the parties». Véase Dobbs, D. (1980). Tortious Interference with Contractual Relationships. *Arkansas Law Review*, 34, 335.

23 17 U.S.C. § 301: «Todos los derechos de origen legal o fundados en la equidad que sean equivalentes a alguno de los derechos exclusivos incluidos en el ámbito general del derecho de autor [ ] o que formen parte del ámbito material del derecho de autor [ ] quedan regulados exclusivamente en este título. En efecto, nadie podrá atribuirse tal tipo de derechos o una facultad equivalente sobre una obra con arreglo al *common law* o a las leyes de un Estado». Véase Bohannan, C. (2008).Copyright Preemption of Contracts. *Maryland Law Review* 67, 611.

24 *Altera Corp. v. Clear Logic, Inc.*, 424 F.3d 1079 (9th Cir. 2005).

implementar estrategias de discriminación de precios, que pueden contribuir a aumentar el bienestar social[25].

También, mediante el derecho de contratos, el titular de los derechos puede diseñar restricciones verticales que le permiten beneficiarse de las ventajas que puede conllevar una situación de integración vertical de la empresa pero sin incurrir en los costes derivados de las reglas de propiedad sobre la organización empresarial[26]. Más que para supuestos de productos dirigidos al público en general, esta idea resulta más relevante para productos destinados a empresarios y profesionales. En este sentido, las restricciones contractuales verticales incentivan a que el distribuidor o transformador del producto realice inversiones específicas, en el marco de un contrato de larga duración, para desarrollar un mercado local y en proporcionar servicios preventa y postventa sin el riesgo de que su principal pueda luego aprovecharse oportunísticamente de las inversiones realizadas.

La confianza en el derecho de contratos y en sus ventajas comparativas, sin embargo, no es ilimitada. El recurso al derecho de obligaciones y contratos encuentra sus fronteras en determinados problemas, algunos de los cuales han sido ya apuntados a lo largo de este trabajo. A continuación, se señalan algunas de las cuestiones principales que plantea el uso del derecho de contratos en la puesta a disposición de productos y servicios relacionados con el entretenimiento online y que deberían plantearse en prevención de contingencias jurídicas derivadas de estos modelos de negocio:

Un primer problema deriva de la falta de un entendimiento sólido y contrastado sobre la interrelación entre derecho de propiedad intelectual y derecho de contratos y, en particular, sobre la cuestión acerca de si mediante una licencia de usuario, unas condiciones de uso predispuestas o, en su caso, un contrato negociado entre las partes se puede alterar sin más el equilibrio de intereses diseñado por el legislador en la regulación sobre derechos de autor. A falta de una norma específica que regule dicha interdependencia en el derecho español, resulta deseable un análisis en profundidad del juego de la autonomía privada en el ámbito de la propiedad intelectual y del carácter imperativo implícito o de orden público que pueden presentar muchas reglas del TRLPI.

En segundo lugar, otro problema reside en la formación del consentimiento en el caso de licencias de usuario o, sobre todo, de condiciones generales de uso de un sitio web o de un

25 La literatura jurídica sobre derechos de autor y discriminación de precios es muy nutrida. Wendy J. Gordon ha propuesto el entendimiento de muchas instituciones propias del derecho de la propiedad intelectual mediante al recurso de la discriminación de precios (Gordon, W. (1998). Intellectual Property as Price Discrimination: Implications for Contract. *Chicago-Kent Law Review*, 73, 1367). Otros desarrollos señalados en la materia incluyen Benkler, Y. (2000). An Unhurried View of Private Ordering in Information Transactions. *Vanderbilt Law Review* 53, 2063; Meurer M. (2001-2002). Copyright and Price Discrimination. *Cardozo Law Review* 23, 55; y Fisher, W. (2007). When Should We Permit Differential Pricing of Information. *UCLA Law Review* 55, 1.

26 Véanse Bar-Gill, O. y Parchomovsky, G. (2009). Law and the Boundaries of Technology-Intensive Firms. *University of Pennsylvania Law Review* 157, 1649; y Barnett, J. (2011). Intellectual Property as a Law of Organization. *Southern California Law Review* 84, 785.

producto o servicio puesto a disposición online, que puede entrañar dificultades adicionales en la aplicación del derecho de contratos[27].

En tercer lugar, la problemática que puede generar el principio de eficacia relativa del contrato para una correcta protección de los incentivos al desarrollo de nuevas obras debe ser examinada y, en particular, el alcance de los mecanismos posibles en derecho español para poder someter al control del titular de los derechos de explotación de una obra a sujetos diferentes de quienes formaron un vínculo contractual con aquél. Relacionado con esta cuestión, deben examinarse, en derecho español, los límites a los actos de competencia desleal por inducción a la infracción contractual (artículo 14.1 LCD).

En cuarto lugar, las diferencias en el régimen de remedios disponibles ante un incumplimiento de una licencia que proporcionan, por un lado, el TRLPI y, por otro, el Código Civil, deben destacarse. Además, la legislación procesal española añade otras diferencias de régimen, como por ejemplo, el régimen de competencia judicial (artículo 86 ter 2.a LOPJ) o de la actividad previa a la demanda encaminada a la obtención de información (artículos 256.1.7 y 256.1.8 LEC).

Finalmente, deben atenderse los límites que puede imponer el derecho de la competencia para salvaguardar actos de abuso en el mercado o actuaciones encaminadas a erigir barreras de entrada para desarrolladores de productos y servicios que puedan ser complementarios a los proporcionados por el titular de los derechos de propiedad intelectual.

Un examen en profundidad de los elementos anteriores contribuirá a determinar, por una parte, hasta qué punto titulares de derechos de autor pueden alterar el equilibrio de intereses diseñado por el legislador sobre propiedad intelectual y cambiar las reglas de su juego gracias al derecho de contratos y a la tecnología y, por otra, hasta qué punto usuarios pueden modificar obras protegidas mediante derechos de autor o desarrollar otras obras o productos complementarios y cambiar, así, las reglas del juego gracias a su afán innovador o a la mera diversión.

4. BIBLIOGRAFÍA

Bar-Gill, O. y Parchomovsky, G. (2009). Law and the Boundaries of Technology-Intensive Firms. *University of Pennsylvania Law Review* 157, 1649.

Barnes, P. (2011). The Prospects for Protecting News Content Under the Digital Millennium Copyright Act. *Harvard Journal of Sports & Entertainment Law* 3, 201.

Barnett, J. (2011). Intellectual Property as a Law of Organization. *Southern California Law Review* 84, 785.

27 Véanse, en este sentido, las Sentencias sobre *screen-scraping* de la Audiencia Provincial de Barcelona, Sección 15ª, de 17 diciembre 2009 (AC 2010\1849). MP: Ignacio Sancho Gargallo. *Ryanair Limited c. Vacaciones eDreams S.L.*; y de 15 diciembre 2009 (AC 2010\1848). MP: Ignacio Sancho Gargallo. *Ryanair Limited c. Atrápalo, S.L.*

Benkler, Y. (2000). An Unhurried View of Private Ordering in Information Transactions. *Vanderbilt Law Review* 53, 2063.

Bohannan, C. (2008).Copyright Preemption of Contracts. *Maryland Law Review* 67, 611.

Carver, B. (2010). Why License Agreements Do Not Control Copy Ownership: First Sales and Essential Copies. *Berkeley Technology Law Journal* 25, 1887.

Determann L. y Fellmeth, A. (2001). Don't Judge a Sale by Its License: Software Transfers Under the First Sale Doctrine in the United States and the European Community. *University of San Francisco Law Review* 36, 1.

Dobbs, D. (1980). Tortious Interference with Contractual Relationships. *Arkansas Law Review*, 34, 335.

Fisher, W. (2007). When Should We Permit Differential Pricing of Information. *UCLA Law Review* 55, 1.

Frischmann, B. (2007). Evaluating the Demsetzian Trend in Copyright Law. *Review of Law and Economics* 3, 269.

Frischmann, B. y Lemley, M. (2007). Spillovers. *Columbia Law Review* 107, 257.

Gordon, W. (1998). Intellectual Property as Price Discrimination: Implications for Contract. *Chicago-Kent Law Review*, 73, 1367.

Hovenkamp, H. (2010). Post-Sale Restraints and Competitive Harm: The First Sale Doctrine in Perspective. *NYU Annual Survey of American Law* 2010, 101.

Katz, A. (2012). What Antitrust Law Can (and Cannot) Teach About the First Sale Doctrine. Disponible en http://ssrn.com/abstract=1845842 (consultado en 24.3.2012).

Lichtman, D. y Landes, W. (2003). Indirect Liability for Copyright Infringement: An Economic Perspective. *Harvard Journal of Law & Technology* 16, 395.

Perzanowski A (2010). Fixing RAM Copies, *Northwestern University Law Review* 104, 1067.

Lemley, M. (2004). Ex Ante versus Ex Post Justifications for Intellectual. Property. *University of Chicago Law Review* 71, 129.

Madison, M. (2003). Reconstructing the Software License. *Loyola University Chicago Law Journal* 35, 275.

Meurer M. (2001-2002). Copyright and Price Discrimination. *Cardozo Law Review* 23, 55.

Shikowitz, R. (2010). Note, License to Kill: *MDY v. Blizzard* and the Battle over Copyright in World of Warcraft. *Brooklyn Law Review* 75, 1015.

Shirky, C. (2010). *Cognitive Surplus: How Technology Makes Consumers Into Collaborators.* New York: Penguin.

Van Houweling, M. (2011). Touching and Concerning Intellectual Property. *Santa Clara Law Review* 51, 1063.

Von Hippel, E. (2005). *Democratizing Innovation*. Cambridge: MIT Press.

EL *SPAM* SOCIAL O ENVÍO PROMOCIONAL NO SOLICITADO A TRAVÉS DE LAS REDES SOCIALES

Trinidad Vazquez Ruano
Profesora Contratada Doctora de Derecho Mercantil de la Universidad de Jaén

RESUMEN: La utilización de nuevas herramientas de comunicación en el ámbito electrónico, como las redes sociales, además de ser de utilidad práctica para los usuarios, también se está convirtiendo en un canal de relevancia de las entidades, en particular como parte de sus campañas promocionales. Los aspectos positivos que caracterizan su utilización y la participación en las mismas se contraponen con actuaciones que pueden resultar contrarias a Derecho. Tal es el caso de la remisión de comunicaciones comerciales de manera indiscriminada y cuando no han sido solicitadas previamente por los destinatarios. Comportamiento que resulta ilícito si se tiene en cuenta la regulación prevista en el art. 21 de la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico, respecto del *envío de comunicaciones publicitarias por correo electrónico u otro medio de comunicación electrónica equivalente*.

Las redes sociales constituyen –en el ámbito electrónico– un eficaz instrumento de comunicación en el que los usuarios facilitan una información de carácter personal de manera directa e indirecta. En este último caso, nos referimos no tanto a los supuestos en los que los datos que se ofrecen afectan al ámbito privado de quien los proporciona, sino que conciernen a otros sujetos que pueden verse perjudicados por las informaciones, imágenes o videos puestos a disposición del público en un determinado perfil, a pesar de que ellos no formen parte de la red social.

La relevancia de esta materia radica en que, como es sabido, la información de los usuarios que se encuentra en el entorno electrónico es de indudable importancia para las entidades, pues permiten crear perfiles concretos de los sujetos y ello, en ocasiones, se hace contraviniendo las disposiciones de la normativa en materia de protección de datos de carácter personal. Por lo que se establece la necesidad de alcanzar un equilibrio que solvente el conflicto de intereses contrapuestos. De un lado, el de las empresas que desean conocer las preferencias de los usuarios a fin de que sus campañas promocionales sean eficientes en un entorno abierto como lo es el de la red Internet; y, de otro, la tutela de la intimidad y de los datos de carácter personal de los sujetos que acceden a la Red con finalidades de diversa naturaleza.

Por ello, tras analizar los aspectos más destacados de la práctica conocida en la actualidad como 'spam social', pretendemos ofrecer algunas recomendaciones que incrementen la confianza y seguridad de los usuarios para que puedan participar en las redes sociales de forma adecuada y en garantía de su privacidad y de la información que les identifica o puede hacerles identificables.

PALABRAS CLAVE: *Spam*, Redes Sociales, Comunicaciones Comerciales, Datos Personales, Nuevas Tecnologías.

1. APROXIMACIONES SOBRE LA MATERIA

La repercusión e importancia que en el ámbito social están teniendo las redes de comunicación electrónicas ha hecho proliferar el número de prestadores que acceden a este medio colectivo con el objeto de dar a conocer al público los productos o servicios que ofertan en un determinado mercado y, en su caso, su propia imagen comercial con la intención de

captar su atención para que, en última instancia, los adquieran o contraten. La participación en las redes sociales electrónicas por parte de las entidades con una finalidad empresarial es sencilla porque sólo requiere el establecimiento de un perfil gratuito y a cambio reporta innumerables ventajas. Ya que constituye una herramienta que permite la fidelización de los clientes y ello hace posible conocer sus intereses y preferencias en tiempo real. Siendo también un medio a través del que se puede recopilar tanto información de los mismos, como quejas o sugerencias que directamente van a remitir los usuarios *on line*.

El problema se plantea porque las posibilidades que ofrecen estos nuevos canales de comunicación hacen que sean utilizados de forma fraudulenta en algunos casos[1]. Tal es el supuesto del envío de mensajes promocionales de manera masiva y que el destinatario no ha consentido. Lo cual, como se ha adelantado, es una práctica prohibida por la norma que prevé la ilicitud de la remisión de mensajes comerciales a través del correo electrónico o medio de comunicación equivalente si previamente no se ha solicitado o autorizado de manera expresa por parte del receptor[2]. Aunque esta restricción general queda exceptuada en los casos en los que la difusión promocional se haga al usuario con el que en un momento previo se ha mantenido una relación contractual de la que se hubieran recabado de manera lícita los datos necesarios para la remisión publicitaria posterior y, además, que la misma se refiera a productos o servicios semejantes con aquellos que fueron objeto de la contratación inicial. En cuyo caso, no se requiere que la entidad anunciante obtenga el consentimiento del receptor de las comunicaciones comerciales para la licitud de su envío.

El legislador ha previsto, asimismo, una exigencia añadida para el prestador del servicio en el ámbito electrónico y es la necesidad de que ofrezca a los usuarios que son destinatarios de sus mensajes publicitarios la opción de poder oponerse al tratamiento de los datos que les conciernen a través de un proceso que les resulte simple y que no le reporte coste alguno[3]. Requerimiento que deberá hacerse efectivo no sólo cuando se recopilen los datos que serán tratados con una finalidad comercial, sino también en cada una de las comunicaciones que se les remitan. En este aspecto, la norma recientemente ha precisado que cuando los mensajes comerciales se difundan a través de las cuentas de correo electrónico, será obligatorio indicar una dirección electrónica correcta con el objeto de que el destinatario pueda ejercer su derecho de oposición a la recepción de comunicaciones de carácter comercial[4]. Estableciéndose, por tanto, la ilicitud de las comunicaciones que siendo promocionales no contengan una válida dirección de correo electrónico a la que el usuario pueda dirigirse. Por cuanto se ha entendido que la forma más simple para que el

1 Siendo algunos ejemplos la difusión de virus electrónicos, la propagación de programas *malware* o de otros mensajes que instalan programas que recogen información personal de modo contrario a Derecho.

2 Art. 21 en su apartado 2º de la LSSIyCE de contenido similar al art. 13 de la Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas, DOUE L 201, de 31 julio).

3 Art. 21. 2º de la LSSIyCE.

4 Modificación introducida por el Real Decreto-ley 13/2012, de 30 de marzo a los arts. 21 y 22 de la LSSIyCE (BOE núm. 78, de 31 marzo).

destinatario de un correo comercial pueda negarse a recibir ulteriores mensajes del mismo tipo va a ser la contestación directa a través de la dirección que se le proporciona.

Si bien, en nuestra opinión, a pesar de la modificación introducida el legislador ha dejado pasar la oportunidad de incluir alguna referencia a otros medios de comunicación similares o equivalentes y que permiten remitir comunicaciones de carácter promocional de manera personalizada, como lo es el terminal telefónico móvil. Habiendo sido deseable añadir alguna mención respecto de la necesaria inclusión de una referencia o contacto válido del emisor para que el destinatario pueda ejercer su derecho de oposición cuando el canal de difusión es similar al correo electrónico (como lo es, por ejemplo, un número de teléfono real).

Estas imposiciones que podemos calificar de especiales y que se establecen respecto de la difusión promocional en el ámbito electrónico responden a la naturaleza personal de los medios o canales por los que se difunden los anuncios y que permiten alcanzar a determinados sujetos, como el correo electrónico u otros similares. Entre los que es posible encuadrar tanto los referidos terminales telefónicos móviles en cuanto al sistema de mensajería corta (*SMS*) o los mensajes multimedia *(MMS)* de contenido promocional[5] como, a su vez, la remisión de mensajes individuales realizados a través de las redes sociales[6]. Pues la creación de un perfil en una red social facilita la comunicación a distancia entre los usuarios de forma masiva en relación con las informaciones que se publican de manera abierta en el muro del perfil. Pero, al mismo tiempo, se permite el envío de comunicaciones privadas a otros miembros que pertenecen a una lista de agregados. En estos supuestos se plantea un agravante, por cuanto no sólo es posible enviar comunicaciones comerciales a específicos sujetos, sino que su contenido puede personalizarse y hacerse individual de acuerdo con los intereses y preferencias de los participantes en la red social a los que se ha hecho un seguimiento sin que, en la mayor parte de los casos, tengan conocimiento de tal circunstancia.

2. EL DENOMINADO *SPAM* EN REDES SOCIALES *('SPAMMING 2.0')* O *SOCIAL NETWORKING SPAM*

La ausencia de una definición taxativa y exacta de la práctica del *spam* hace que –a efectos de la determinación de su contenido– nos ocupemos de los aspectos que singularizan

5 Sobre ello, GUILLÉN CATALÁN, R. (2010), La protección de los destinatarios de *SPAM* a través de la telefonía móvil: una visión práctica, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 23, 35-45. Incluso, en algunos casos, hemos incluido en esta previsión la remisión de anuncios comerciales emergentes que aparecen de modo sorpresivo cuando se visitan determinados espacios (*pop ups*). Vid., VAZQUEZ RUANO, T. (2008), *La protección de los destinatarios de las comunicaciones comerciales electrónicas*, Madrid, Marcial Pons y en (2010), El *spam* y la nueva regulación de la Ley de Competencia Desleal, *Revista de Derecho Mercantil,* 277, 1083-1101.

6 Véase GUILLÉN CATALÁN, R. (2005), *Spam y comunicaciones comerciales no solicitadas*, Pamplona, Aranzadi, 115. Como se prevé en el art. 9 del Código Ético de Comercio Electrónico y Publicidad Interactiva (en: http://www.confianzaonline.es/Codigo_CONFIANZA_ONLINE.pdf) que de forma expresa se ocupa de *(...) la publicidad enviada al correo electrónico u otros medios de comunicación individual equivalentes (...)*.

esta forma de difusión promocional. En razón de los cuales podemos afirmar que se refiere a la remisión de mensajes comerciales que no se ha consentido y que se lleva a cabo por canales de comunicación electrónicos que alcanzan a determinados destinatarios. Pues, a diferencia de otros textos normativos, en el marco jurídico español es el consentimiento o la autorización individual del sujeto destinatario el condicionante que determina la licitud del ejercicio promocional[7]. No haciéndose referencia al aspecto cuantitativo ni cualitativo del término y calificándose como infracción grave *el envío masivo de comunicaciones comerciales a destinatarios que no lo hayan autorizado o no se hayan opuesto a ello o de más de tres en el plazo de un año al mismo destinatario*[8].

En consecuencia, a diferencia del simple *mailing*, el *spamming* se caracteriza porque la naturaleza de su contenido es promocional, encuadrándose así en la actividad de empresa. Por su parte, el *social networking spam* o también denominado *spam* social se concreta en la difusión de comunicaciones comerciales no solicitadas que se distribuyen por un determinado canal de interrelación de los usuarios a distancia, cual es la red social electrónica.

En este sentido, consideramos que las redes sociales pueden ser utilizadas por parte de las entidades para publicitarse o promocionar los productos o servicios que ofrecen en el mercado en una doble vertiente. De un lado, de forma colectiva o genérica, es decir que la entidad crea su propio perfil social y a través del mismo va a difundir comunicaciones comerciales de forma colectiva. Aunque, cabe también una segunda alternativa y es la remisión de mensajes privados o individualizados que sólo van a alcanzar a sujetos que se han determinado de modo intencionado. Siendo esta segunda posibilidad la que plantea en la práctica diversas cuestiones en razón de la tutela de la información de carácter personal y de la intimidad de los usuarios que pertenecen a la red social, como tendremos ocasión de comprobar en el epígrafe siguiente.

---

7 Nuestra norma responde a las previsiones de los textos comunitarios, en concreto los arts. 6 y 7 de la Directiva 2000/31/CE, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico, DOUE L 178, de 17 julio) y el art. 13 de la Directiva 2002/58/CE en materia de envío de mensajes electrónicos con fines de venta directa. Distinto es el caso de la *Can Spam Act* –Secciones 2 a 8– (*the final text of S. 877 as it was passed by the Senate on 25 november 2003, and agreed to by the House of representatives on 8 december 2003, appears below. The bill was signed by the President on 16 december 2003, and takes effect on 1 january 2004*, en: http://www.spamlaws.com/federal/108s877.html) en el marco norteamericano que se ocupa de las comunicaciones electrónicas cuyo contenido resulta engañoso, falso o contrario a Derecho, pudiendo ser de carácter comercial o no.

8 Según lo dispuesto en el art. 38. 3º b) de la LSSIyCE, aunque si no puede encuadrarse entre las infracciones graves se entenderá que es de carácter leve (como sucede en la resolución de la AN, Sala de lo contencioso- administrativo, Secc. 1ª, de 15 julio 2011, en cuyo caso el envío de comunicaciones comerciales a un cliente y, además, accionista sin haber manifestado su consentimiento se califica como infracción leve porque en cada una de las comunicaciones remitidas se facilita la posibilidad de oponerse a ello, –Recurso 256/2010. SP/SENT/640580–). De acuerdo con el art. 39 de la LSSIyCE la comisión de infracciones graves se sancionará con multas cuya cantidad oscilará entre los 30.001 a los 150.000 euros, mientras que para las infracciones leves se prevé que podrá ser de hasta 30.000 euros.

La regulación nacional prevista respecto de la difusión de comunicaciones electrónicas de contenido promocional ha establecido la necesidad de atender y respetar las normas vigentes en la materia (en particular, en el ámbito comercial y publicitario[9]) y de una forma especial las que se ocupan de la garantía de los datos de carácter personal[10]. Si bien, a continuación, se recogen unos presupuestos de necesario cumplimiento para la difusión publicitaria a través de diversos canales electrónicos. El primero de ellos es de carácter general en cuanto que se refiere a la necesidad de que las comunicaciones comerciales remitidas sean claramente identificables como tales, indicando a su vez la persona física o jurídica en nombre de la cual se realizan[11]. Especificándose que en los casos en los que la publicidad se distribuya por medios como el correo electrónico o similares deberá incluirse al inicio de la misma la palabra '*publicidad*' o la abreviatura *publi*. Esta última apreciación entendemos que responde a la remisión de comunicaciones promocionales de contenido limitado como sucede cuando se envían mensajes cortos publicitarios a los terminales telefónicos móviles.

En consecuencia, el legislador ha previsto la prohibición de las comunicaciones que se envíen sin que se determine la identidad del sujeto que las remite o en las que se oculte la misma, al igual que las que provoquen a los receptores a acceder a páginas electrónicas que incumplan las previsiones normativas mencionadas[12].

Completando esta exigencia genérica de identificación se establece una especialidad respecto de las comunicaciones comerciales que se difunden a través de medios como el correo electrónico o equivalentes. En cuyo caso, como se ha referido anteriormente, se impone la necesidad de recabar el consentimiento de los destinatarios de las mismas antes de su remisión y que deberá ser expreso, salvo que hubiese mediado una relación contractual previa de la que el prestador haya obtenido lícitamente los datos que permiten el envío publicitario posterior y que los productos o servicios promocionados guarden relación con aquellos que fueron objeto de la contratación[13]. Del mismo modo, se exige que el prestador proporcione al destinatario de las comunicaciones promocionales la facultad de ejercer su derecho de oposición al tratamiento de la información que le concierne habilitando para ello un procedimiento simple y gratuito. En este sentido, se prevé de modo expreso la presunción de una válida cuenta de correo electrónico como mecanismo sencillo para que el receptor pueda ejercer su derecho de oposición a recibir de nuevo mensajes promocionales a través de ese mismo canal de comunicación.

De acuerdo con lo expuesto, la difusión publicitaria que se lleva a cabo por medio de las redes sociales ha de cumplir con las previsiones normativas aplicables al ámbito comercial

9 Según lo dispuesto en el art. 19 de la LSSIyCE.

10 Ley 15/1999, de 13 diciembre de protección de datos de carácter personal (BOE núm. 298, de 14 de diciembre, en adelante LOPD) y su Reglamento de desarrollo (RD 1720/2007, de 21 de diciembre, BOE núm. 17, de 19 de enero).

11 Art. 20. 1º de la LSSIyCE.

12 Modificación introducida por el Real Decreto-ley 13/2012, de 30 de marzo.

13 El texto de la Directiva 2002/58/CE concreta que la dirección se hubiera obtenido 'en el contexto de la venta de un producto o servicio'.

y publicitario y, en todo caso, respetar el deber de estar claramente identificada como tal al igual que la entidad anunciante desde cuyo perfil o en cuyo muro se remiten los mensajes comerciales. Es decir, que en el mensaje que se publique se incluya la referencia de que se trata de una promoción o que el contenido es publicitario.

Por su parte, respecto a los supuestos en los que la entidad se valga del perfil que tiene creado en una red social para enviar mensajes promocionales individualizados a los sujetos agregados –junto al necesario cumplimiento de los presupuestos normativos de protección de los datos de carácter personal como se analizará en el epígrafe siguiente[14]– tendrá la obligación de obtener de los mismos su expreso consentimiento. A menos que hubieran sido clientes de la entidad en un momento anterior y que de dicha relación contractual se hubieran obtenido los datos de contacto de forma lícita y el contenido de la publicidad se refiera a productos o servicios similares a los contratados inicialmente. Este último caso, puede plantear ciertas dudas interpretativas. En tanto que, siguiendo el contenido de la norma sobre protección de datos de carácter personal, es necesario cancelar los datos cuando hayan dejado de ser necesarios o pertinentes para la finalidad que justifica su obtención[15]. Lo que lleva a considerar que cuando de nuevo se pretendan usar con fines promocionales los datos de los sujetos que mantuvieron una relación jurídica con la entidad sea preciso que se vuelva a recabar su consentimiento para la remisión de las comunicaciones promocionales en los términos indicados y de manera lícita.

Sin embargo, en un sentido opuesto, también es posible entender que cuando la información personal se recopila con una finalidad comercial y con el objeto de realizar campañas publicitarias, la finalidad va a ser duradera o prolongada en el tiempo y, por ende, no sería preciso obtener en cada ocasión la voluntad del receptor de los mensajes promocionales. Al menos, en los supuestos en los que el contenido comercial sea similar a aquél que fue objeto de la contratación inicial, como se ha advertido. Siendo esta segunda alternativa la que consideramos que va a resultar más afín con la práctica empresarial.

3. LA TUTELA DE LA INFORMACIÓN DE CARÁCTER PERSONAL EN LAS REDES SOCIALES

3.1. Presupuestos generales en materia de protección de datos

El respeto de la normativa en materia de protección de la información de carácter personal, como se ha señalado, es una exigencia que de manera explícita ha previsto el legislador en cuanto a la remisión de comunicaciones comerciales a través de canales electrónicos que alcanzan a determinados sujetos. Lo cual, entendemos, trae su causa en las dos fases o mo-

14 *Infra 3.- La tutela de la información de carácter personal en las redes sociales.*

15 Se permite que la información de los clientes se deje bloqueada durante cierto tiempo por si se exigiese algún tipo de responsabilidad derivada de la relación jurídica o de la ejecución del contrato inicial o, en su caso, de la aplicación de medidas precontractuales solicitadas por el interesado (arts. 4 y 16 de la LOPD).

mentos que caracterizan la difusión publicitaria por medios electrónicos de carácter personal como el correo electrónico, el terminal telefónico móvil o el perfil de un sujeto en una red social[16]. En primer término, la etapa inicial que se corresponde con la de recopilación y tratamiento de los datos personales y que resulta necesaria para el posterior envío de los mensajes promocionales a los destinatarios[17]. Y que, en ciertos supuestos, también se emplean para concretar el perfil de los receptores y determinar el contenido de las comunicaciones que se les van a enviar. Superada esta primera etapa, en segundo lugar, procede la que podemos denominar de ejecución propiamente dicha o de remisión de las comunicaciones comerciales antes referidas. En la que se prevé como requisito necesario haber obtenido el consentimiento expreso o autorización por parte de los destinatarios para que sea considerada una remisión promocional acorde a Derecho, salvo el supuesto excepcional antes referido[18].

Ocupándonos de la primera fase mencionada se hace necesaria la observancia y cumplimiento de los presupuestos recogidos en la norma de protección de datos de carácter personal[19]. En cuyo caso, se impone la necesidad de obtener del interesado el consentimiento tanto para la recopilación, como para el almacenamiento y posterior tratamiento de la información que le concierne, a menos que legalmente se hubiere previsto lo contrario[20]. A tal fin, se establece que sea una manifestación de la voluntad *inequívoca* en cuanto a la obtención de datos básicos o, lo que es lo mismo, informada[21]. En razón de lo cual se considera esencial

16 Sobre esta materia VÁZQUEZ RUANO, T. (2012), La tutela de la información personal y el uso de las redes sociales, *Universitas. Revista de Filosofía, Derecho y Política*, 15, 125-147.

17 Como se ha previsto en la *Comunicación de la Comisión Europea sobre las comunicaciones comerciales no solicitadas o spam*, (2004), en: http://europa.eu/legislation_summaries/information_society/internet/l24190a_es.htm (comentada por GAUTHRONET, S/ DROUARD, E.), Bruselas, 4-5 y 9. De interés son también los trabajos de MESSÍA DE LA CERDA BALLESTEROS, J. A. (2004), *La protección de datos de carácter personal en las telecomunicaciones,* Madrid, Dykinson, 178-179; RIVERO GONZÁLEZ, Mª D. (2003), Régimen jurídico de la publicidad en Internet y las comunicaciones comerciales no solicitadas por correo electrónico, *Revista de Derecho Mercantil,* 250, 1596 y en (2005), *Revista de Autocontrol de la Publicidad,* 93, 24-38.

18 Art. 21 de la LSSIyCE.

19 De acuerdo con lo previsto en el Título II relativo a los *Principios de la protección de datos* (arts. 4 a 12) y en el Título III sobre los *Derechos de las personas* (arts. 13 a 19) de la LOPD. Lo cual se relaciona con los arts. 6, 7, 14, 16, 17 de la Directiva 95/46/CE y los arts. 4, 5, 6, 9 y 15 de la Directiva 2002/58/CE. Para ampliar esta materia pueden consultarse, entre otros, ARENAS RAMIRO, M. (2006), *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant Lo Blanch, 303-307; FERNANDO MAGARZO, Mª R. (2003), La protección de datos personales en el ámbito de la publicidad, *Revista de la Asociación de Autocontrol de la Publicidad*, 77, 30-31; SERRANO PÉREZ, Mª. M. (2003), *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid, Thomson- Civitas, 78-80.

20 Art. 6 de la LOPD y arts. 14- 15 del RLOPD, pudiendo ser un consentimiento expreso o tácito porque la norma no concreta su forma. El responsable del tratamiento tiene que atender los presupuestos de seguridad exigidos para lo que será preciso que adopte las medidas técnicas y organizativas que garanticen la seguridad de los datos.

21 Distinta consideración cabe hacer respecto de los supuestos en los que se proporcionen datos que ostentan la categoría de especialmente protegidos (origen racial, la salud y la vida sexual) en los que se

el principio de calidad de los datos, el de seguridad en el tratamiento y el de información al interesado sobre el sujeto que los obtiene, los datos que se recopilan y que serán adecuados, pertinentes y necesarios; y la finalidad que lo justifica[22]. Precisándose que dichos datos sean obtenidos de manera adecuada y sin haber empleado medios fraudulentos, desleales o contrarios a Derecho; debiendo actualizarlos cuando corresponda y no pudiendo conservarse durante un tiempo excesivo. Así, cumplido el objetivo que determinó su recogida y tratamiento, la información personal ha de ser eliminada o, en su caso, bloqueada[23].

No obstante, la LOPD recoge un supuesto concreto de tratamiento de información de carácter personal con una finalidad promocional[24], estableciendo la posible utilización de la misma cuando se hubiere recopilado con fines comerciales de fuentes accesibles al público o si los ha facilitado el receptor o ha manifestado en un momento previo su consentimiento para ello. A este respecto, hay que tener en cuenta que a pesar de que la norma delimita las fuentes consideradas de acceso público[25], no es menos cierto que se presume el consentimiento del interesado al permitir que las entidades anunciantes recopilen de una fuente accesible al público los datos necesarios para ello sin que éste haya otorgado su conformidad. Por lo que, en principio, la difusión publicitaria en el marco de una actividad empresarial va a justificar la obtención de los datos de los receptores sin necesidad de su consentimiento cuando se trate de clientes de la misma. Siempre que ello no suponga una vulneración de los derechos y libertades fundamentales del interesado[26].

Asimismo, la norma reconoce un conjunto de facultades específicas que se le reconocen al titular de la información personal y que éste va a poder ejercer respecto de la misma[27]. Nos referimos al derecho de acceso a la información almacenada, el de rectificación o de cancelación cuando hubiera dejado de ser necesaria o pertinente para la finalidad que determinó su obtención o registro; la oposición al tratamiento siempre que medie causa justificada y

---

requiere consentimiento expreso (art. 7. 3º de la LOPD) y si se trata de datos de ideología, afiliación sindical, religión y creencias se precisa también que sea por escrito (art. 7. 2º de la LOPD). El RLOPD, además, exige al responsable del tratamiento que *compruebe* la edad del menor y la autenticidad de su consentimiento o el de sus padres o tutores, pues en el caso de que sea un menor el que vaya a facilitar sus datos para acceder a una red social (art. 13). Cuando sean menores de catorce años, será necesario en todo caso el consentimiento de padres o tutores. Los que sean menores, pero mayores de catorce años podrán dar su consentimiento, salvo que la ley exija que padres o tutores asistan en la prestación del consentimiento.

22 Arts. 4-6 de la LOPD y art. 8 del RLOPD.

23 Lo que supone la posibilidad de acceder a los mismos que se mantiene para las administraciones públicas, jueces y tribunales en razón de posibles responsabilidades. Pero prescrito el plazo de reclamación de las mismas, tendrán que ser definitivamente eliminados de los ficheros.

24 Según lo dispuesto en el art. 30 de la LOPD.

25 Art. 3, letra j) de la LOPD.

26 De acuerdo con el art. 6 de la LOPD.

27 Véanse los arts. 4. 5, 6.4 y 30.4 de la LOPD y los arts. 27-36 del RLOPD. Así como los arts. 12 a 14 de la Directiva 95/46/CE.

sin que ello le reporte coste económico alguno; el derecho de consulta gratuita al Registro General de Protección de Datos y la posibilidad de impugnar las valoraciones para no sentirse afectado por actos administrativos o decisiones privadas que generen el análisis de sus conductas al objeto del tratamiento de datos que sólo definan su personalidad.

3.2. Especialidades de la tutela de los datos personales del usuario de una red social

En lo que concierne a las redes sociales, hay que tener en cuenta que el usuario facilita inicialmente una información básica al objeto de poderse registrar y crear su perfil en la misma para participar junto al resto de miembros. Lo cual hace de manera voluntaria y siendo consciente de que esos datos se van a poner a disposición de los participantes de la red social (según la configuración). Sin embargo, en nuestra opinión, estos canales de comunicación e interrelación electrónicos van más allá en materia de protección de los datos de carácter personal[28]. Por cuanto no sólo se ofrece información que afecta directamente a la esfera privada del que tiene creado un perfil en la red, sino que –como se ha adelantado– indirectamente esa información puede pertenecer a otros sujetos. Los cuales, en algunos casos, ni siquiera forman parte de la red social. Pues el usuario no facilita únicamente unos datos de registro al inicio, sino que de manera continua y habitual va actualizando la información, incluyendo imágenes, videos, enlaces y otras referencias que aluden a su esfera privada y a la de terceros (aún cuando ello se desconoce) que lo debieran haber autorizado[29]. No teniendo conocimiento del alcance y repercusión que la inclusión de esos datos o información posee en un entorno como el electrónico[30]. En consecuencia, como se ha dicho, se genera un riesgo mayor para la tutela de la intimidad y de los datos de carácter personal.

La ingente cantidad de información que identifica o, en su caso, puede hacer identificable a los sujetos y que circula en las redes sociales es de indudable importancia para las entidades que acceden a este nuevo medio con una finalidad promocional. Y que no sólo van a preocuparse de obtener datos de contacto de los miembros de la misma para hacerles llegar sus comunicaciones comerciales, sino que además van a tratar de conocer gustos, preferencias e intereses a fin de adecuar el contenido de sus promociones para que resulten más eficientes. Lo que suele llevarse a cabo, en la mayor parte de las ocasiones, empleando técnicas que incumplen los presupuestos normativos en materia de protección de la información que pertenece a los sujetos referidos[31].

---

28 Como ya indicábamos en trabajos anteriores, VÁZQUEZ RUANO, (2012), *op.cit.,* 125-147.

29 Véase la *Resolución sobre Protección de la privacidad en los servicios de redes sociales*, *30ª Conferencia Internacional de Autoridades de Protección de Datos y privacidad*, (2008), Estrasburgo, 1-2, en: http://www.agpd.es/portalwebAGPD/ canaldocumentacion/conferencias/common/pdfs/30_conferencia_internacional/resolucion_redes_sociales.pdf).

30 Siendo habitual que la información sea tratada y, además, cedida a terceros sin su conocimiento. Tal y como se ha puesto de manifiesto en la *Resolución sobre Protección de la privacidad en los servicios de redes sociales*, *op.cit.*, 3-4.

31 VÁZQUEZ RUANO, (2008), *op.cit.*, *passim.*

Una de las prácticas habituales a este respecto es que la entidad que desea promocionarse usurpe la identidad de terceros agregados en el perfil de un sujeto y que no se ha autorizado. Lo que implica que el perjuicio causado afecte a un mayor número de personas, pues los usuarios –en la creencia de que se trata de uno de los sujetos que tienen agregados– van a confiar en ellos en mayor medida. Así como también que la entidad se inmiscuya de manera ilegítima o fraudulenta en un determinado perfil para obtener información concerniente a una determinada personal y que luego empleará, por ejemplo, para remitirle comunicaciones comerciales que no se han solicitado.

A ello hay que añadir que –dependiendo de la política de privacidad y de las pautas de funcionamiento de la red social–, pese a que lo normal es que lo publicado en el muro personal de un participante o miembro únicamente esté disponible para el grupo de sus agregados, no siempre sucede así. Siendo posible en algunas redes sociales que cualquier persona que acceda a la misma esté habilitada para visualizar el contenido publicado por los demás, con independencia de que se encuentre agregado o no a su perfil[32]. Lo que va a traer como consecuencia que se amplíen sus posibilidades de actuación tanto respecto de la distribución de mensajes de naturaleza promocional, cuanto de cualquier otro tipo de fraude o conducta ilícita por medios electrónicos.

En definitiva, como poníamos de manifiesto desde el inicio, consideramos que la práctica del *spam* social o la remisión promocional no solicitada a través de las redes sociales se encuentra directamente relacionada con la tutela de la información de carácter personal. En el sentido de que se trata de un medio de comunicación e interrelación electrónico que se halla vinculado con un determinado sujeto y en el que es factible disponer de una importante cantidad de datos e informaciones sobre el mismo que, aunque en un principio y consideradas de manera aislada no identifican a un determinado sujeto, relacionadas entre sí pueden hacerlo identificable. Afectando de este modo a su esfera privada o personal y, en su caso, a la de terceros.

A igual conclusión cabe llegar si tenemos en cuenta que para remitir mensajes comerciales electrónicos que no se han solicitado o, en su caso, de cualquier otro contenido contrario a Derecho, los prestadores suelen simular identidades que no se corresponden con la realidad, perjudicando con ello a los participantes en la red social y vulnerando su privacidad y la garantía de la información que les concierne.

4. IDEAS FINALES. POSIBLES RECOMENDACIONES

Expuestas las ideas anteriores, parece que lo que podría ser un recurso de indudable relevancia para que las entidades se dieran a conocer de forma eficiente en el entorno electrónico y de utilidad para interactuar con los usuarios, en ocasiones se torna en sentido negativo. Pues su uso fraudulento o contrario a Derecho desvirtúa las ventajas que a priori podría

32 Es el caso, por ejemplo, de la red social *Pinterest*.

aportar a las entidades. No sólo por su empleo como canal de difusión publicitaria masiva y no autorizada, sino también de ejecución de prácticas como *phishing,* distribución de virus u otro contenido ilícito. Por ello, entendemos que es preciso establecer determinadas propuestas a fin de que las entidades puedan recurrir a este canal de comunicación con los usuarios con una finalidad comercial y hacerlo de manera efectiva[33].

La primera idea que cabe poner de manifiesto es la necesidad de que la entidad cree su propio perfil en la red social el cual, al ser de naturaleza comercial deberá estar claramente identificado como tal. A efectos de que los sujetos interesados en la misma o en sus productos o servicios se agreguen y tengan la posibilidad de interactuar con la entidad de que se trate. Así las comunicaciones comerciales que se hagan públicas en el muro de la entidad serán aceptadas por ellos, permitiéndoles conocer las promociones cuando deseen.

Por su parte, en el supuesto de que se pretendan individualizar los mensajes comerciales va a ser preciso no sólo atender a las disposiciones normativas en materia publicitaria y comercial, sino también lo dispuesto en la LSSIyCE en cuanto a la remisión promocional por medios electrónicos y al contenido específico de la LOPD respecto de la tutela de la información de carácter personal. Por lo que, en el caso de los sujetos agregados al perfil de la entidad, resultará suficiente con que ésta contactase directamente a través de la red social con el sujeto interesado en sus productos o servicios y le informe de la posible remisión de comunicaciones comerciales sobre los mismos. O, en su caso, cuando se trate de sujetos que son clientes de la entidad esta información se hará en el momento en el que se contrate un servicio o adquiriese un bien. Indicándole la posible remisión de mensajes comerciales por medio de las redes sociales en un momento posterior a fin de obtener el consentimiento preciso. En cualquier caso, como se ha indicado, debe ofrecerse al usuario tanto al inicio, como en cada una de las comunicaciones comerciales electrónicas que se le remitan, la posibilidad de oponerse a ello mediante una válida dirección de correo electrónica u otro mecanismo similar que resulte sencillo y sin que le reporte ningún coste.

Sin embargo, mayores dudas plantea el cumplimiento de la normativa en materia de protección de datos. Pues estas exigencias jurídicas tienen que respetarse y cumplirse desde el inicio. Es decir, que será en el formulario inicial que el usuario de la red cumplimente para formar parte de la misma y crear su perfil social, como a posteriori donde se haga referencia a la información y extremos contenidos en la normativa de protección de datos[34]. Ofreciendo los mecanismos necesarios para que los usuarios puedan oponerse no sólo a recibir mensajes comerciales que no han solicitado, sino también al tratamiento de la información que les concierne con una finalidad comercial. Siendo esencial que se incluya un enlace permanente con la política de privacidad o extremos de protección de datos en el que se adviertan los pre-

33 Vuélvase de nuevo sobre la *30ª Conferencia Internacional de Autoridades de Protección de Datos y privacidad*, *op.cit.*, 4-5 y el *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*, *op.cit.*, 15-16.

34 Consúltense las recomendaciones del *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*, *op.cit.*, 166-172.

supuestos jurídicos en materia de protección de datos y, de manera específica, de la necesidad de obtener el consentimiento de terceros en el caso de que se vean afectados por la publicación de información, imágenes, videos u otras referencias en un muro o perfil de la red social.

El cumplimiento de los aspectos indicados consideramos que va a hacer que las redes sociales puedan emplearse por parte de las entidades como medios o canales de interacción con los clientes y que, en última instancia, les va a reportar beneficios en el ámbito empresarial. Por cuanto la seguridad y confianza proporcionada a los usuarios de estas herramientas electrónicas de comunicación se halla directamente vinculada a su utilización eficiente.

5. BIBLIOGRAFÍA

5.1. Referencias bibliográficas

Arenas Ramiro, M. (2006), *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant Lo Blanch.

Fernando Magarzo, Mª R. (2003), La protección de datos personales en el ámbito de la publicidad, *Revista de la Asociación de Autocontrol de la Publicidad*, 77.

Guillén Catalán, R. (2010), La protección de los destinatarios de *SPAM* a través de la telefonía móvil: una visión práctica, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 23.

Messía de la Cerda Ballesteros, J. A. (2004), *La protección de datos de carácter personal en las telecomunicaciones,* Madrid, Dykinson.

Rivero González, Mª D. (2003), Régimen jurídico de la publicidad en Internet y las comunicaciones comerciales no solicitadas por correo electrónico, *Revista de Derecho Mercantil,* 250; y en (2005), *Revista de Autocontrol de la Publicidad,* 93.

Serrano Pérez, Mª. M. (2003), *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid, Thomson- Civitas.

Vázquez Ruano, T. (2008), *La protección de los destinatarios de las comunicaciones comerciales electrónicas*, Madrid, Marcial Pons.

– (2010), El *spam* y la nueva regulación de la Ley de Competencia Desleal, *Revista de Derecho Mercantil,* 277.

– (2012), La tutela de la información personal y el uso de las redes sociales, *Universitas. Revista de Filosofía, Derecho y Política*, 15.

5.2. Recursos normativos

Can Spam Act (*takes effect on 1 january 2004*, en: http://www.spamlaws.com/federal/108s877.html).

Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas, DOUE L 201, de 31 julio).

Directiva 2000/31/CE, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico, DOUE L 178, de 17 julio).

Comunicación de la Comisión Europea sobre las comunicaciones comerciales no solicitadas o spam, (2004), en: http://europa.eu/legislation_summaries/information_society/internet/l24190a_es.htm (comentada por GAUTHRONET, S/ DROUARD, E.), Bruselas.

Ley 15/1999, de 13 diciembre de protección de datos de carácter personal (BOE núm. 298, de 14 de diciembre, LOPD).

Real Decreto 1720/2007, de 21 diciembre, de desarrollo de la Ley orgánica de protección de datos de carácter personal (BOE núm. 17, de 19 de enero, RLOPD).

Ley 34/2002, de 11 julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (BOE núm. 166, de 12 julio, LSSIyCE).

Código Ético de Comercio Electrónico y Publicidad Interactiva (en: http://www.confianzaonline.es/Codigo_CONFIANZA_ONLINE.pdf).

Real Decreto-ley 13/2012, de 30 marzo, que transpone al ordenamiento Directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista (BOE núm. 78, de 31 marzo).

5.3. Otros recursos

Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, *Agencia Española de Protección de Datos de carácter personal (AEPD) y el Instituto Nacional de Tecnologías de la Comunicación (INTECO)*, 2009, en: http://www.inteco.es/Seguridad/Observatorio/ Estudios/est_red_sociales_es.

Resolución sobre Protección de la privacidad en los servicios de redes sociales, *30ª Conferencia Internacional de Autoridades de Protección de Datos y privacidad*, 2008, Estrasburgo, en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/30_conferencia_internacional/resolucion_redes_sociales.pdf).

COMUNICACIONES SOBRE GOBIERNO Y POLÍTICAS REGULATORIAS

DEMOCRACIA ELECTRÓNICA, INTERNET Y GOBERNANZA. UNA CONCRECIÓN

Fernando Galindo Ayuda
Catedrático de Filosofía del Derecho de la Universidad de Zaragoza

RESUMEN: El trabajo presenta una reflexión práctica sobre el alcance y los límites que tienen, desde una perspectiva jurídica, los usos democráticos en Internet, atendiendo a: 1) las afirmaciones básicas que sobre democracia se hace en los textos políticos, 2) el significado e implicaciones de algunas de las prácticas propiciadas por el uso de Internet a las que se viene caracterizando como democráticas, y 3) la presentación de algunas experiencias que promueven la participación de los usuarios de Internet en el conocimiento de las actividades de las instituciones públicas.

PALABRAS CLAVE: Democracia. Internet. Gobernanza. Acceso a la información. Open data. Observatorio. Inclusión digital. Gobierno electrónico.

1. INTRODUCCIÓN[1]

La expresión democracia aparece reiteradamente en Internet. Y ello no sólo (1) en lo relativo a la acumulación de información sustantiva, es decir: definiciones, expresiones, teorías y conceptos, que sobre democracia se hace en la red, entendiéndola como término que ayuda a caracterizar a aquellos regímenes políticos en los que los ciudadanos eligen a sus representantes y con ello participan en el proceso de gobierno público, sino también (2) en lo que se refiere a la relación existente entre Internet y democracia, entendiendo que el funcionamiento de la misma Internet o la «red» es democrático o propicia la democracia, al

1 Este trabajo se desarrolla en el marco de los siguientes proyectos: *Establecimiento en Iberoamérica del Observatorio de Gobierno Electrónico. EGOBS, Acción integrada para el fortalecimiento institucional*, financiada por la Agencia Española para la Cooperación Internacional al Desarrollo (AECID), 2009-2012; *La nueva ecología de la información y la documentación en la sociedad del conocimiento: desarrollo de una métrica sistémica, planificación de un observatorio para su seguimiento e identificación de tendencias básicas y retos estratégicos (infoscopos.com)*, proyecto financiado por la CICYT 2010-2012, y *Mejora en la participación en la sociedad del conocimiento a través de las actividades del Observatorio de Gobierno Electrónico. Aspectos políticos, económicos y empíricos*, financiado por la Secretaría General de Universidades, Ministerio de Educación, Cultura y Deportes, convocatoria para la concesión de subvenciones para la cooperación interuniversitaria con Brasil, 2012-2013. El trabajo es un desarrollo de posiciones cuyas bases quedaron establecidas en: Galindo, F. (2011). Democracia electrónica, Internet y gobernanza. *Derecho y Tecnología*, 109-125, y Galindo, F. (2011). Electronic democracy and governance. En Kleve, P. Van Noortwijk, (eds.), *Something bigger than yourself: Essays in honour of Richard de Mulder* (41-56). Rotterdam: Erasmus University.

considerar que facilita a todo el que la maneja, en definitiva al que cuenta con un medio de acceso a la misma un conocimiento/poder/dominio sobre la realidad que antes no lo tenía: estaba reservado a quien había sido nombrado «gobernante» en el proceso de elección democrática de representantes políticos. En el presente trabajo discurrimos sobre estas cuestiones clarificando, especialmente, el alcance del segundo de los aspectos, contrastándolo con el primero, es decir averiguando la efectiva potenciación de la democracia, entendida como participación política, que genera el uso de Internet.

A estos efectos aportamos en forma resumida, en primer lugar (2), consideraciones generalmente aceptadas sobre democracia y participación política que se producen en la actualidad, a efectos de comprender sus implicaciones. En segundo lugar (3) mostramos algunos ejemplos reales de potenciación de la democracia y de las instituciones que se ponen en práctica mediante el uso de Internet. En tercer lugar (4) recogemos algunas consideraciones sobre el hecho de que el acceso a Internet, y por su medio el acceso a información, no implica tanto el incremento de la participación política cuanto que de la comunicación. En cuarto lugar (5) nos fijamos en la relevancia de la denominada brecha digital como obstáculo a un hipotético ejercicio de la democracia participativa por los ciudadanos usando Internet. En quinto lugar (6) prestamos atención a determinadas iniciativas que potencian una efectiva realización de la democracia mediante el uso de Internet, asumiendo que democracia es, también, participación de ciudadanos informados en la actividad pública. En sexto lugar (7) concluimos.

2. DEMOCRACIA HOY

Un sistema político democrático es el que está organizado atendiendo a (1) la garantía e impulso de tres mecanismos, hoy principios jurídicos fundamentales, reconocidos en las constituciones y hechos realidad en la vida diaria de los países donde las mismas funcionan, y (2) la satisfacción de un requisito previo para el ejercicio de mecanismos y principios: el acceso a información. En el presente apartado nos referimos a estos requisitos así como (3) a la gobernanza en cuanto, como veremos, esta es la principal política o filosofía que rige hoy la puesta en práctica por los poderes públicos de mecanismos, principios y acceso a información.

2.1. Los principios jurídicos fundamentales

Son los referidos a la libre elección de los gobernantes por los ciudadanos, la efectiva puesta en práctica de la división del ejercicio del poder político por las instancias de gobierno competentes, y la salvaguarda de la protección y promoción[2] de los derechos humanos por

2 Sobre el papel activo del Estado en la promoción de derechos más que en la simple protección, véase, por ejemplo, Carbonell, M. (2008). Constitution's functionality and social rights: outline of some problems. *Estudios Constitucionales, 6* (2), 43-71

los poderes públicos con respecto a las actividades que tienen lugar en el desarrollo de la vida propia de los ciudadanos.

Los tres mecanismos son considerados propios del funcionamiento del Estado de Derecho. Su contenido y función característicos son resumidos a continuación.

El primer mecanismo es el de la libre elección de los gobernantes por los ciudadanos, que se pone en práctica mediante la realización de procesos electorales que permiten a todos los ciudadanos participar en el gobierno nombrando periódicamente a sus representantes en distintos ámbitos políticos de decisión. Este procedimiento participativo, democrático, se ve completado por la posibilidad que tienen los ciudadanos de intervenir en las actividades gubernamentales mediante la puesta en realidad de otros medios como el referéndum con relación a cuestiones concretas sometidas a opinión de la ciudadanía por los representantes políticos, la coparticipación en actividades de carácter gubernamental mediante la intervención de ciudadanos cuya actuación está prevista en la regulación de procedimientos administrativos, y la participación de los ciudadanos en la solución de conflictos por los tribunales de justicia mediante su intervención como jurados.

El segundo mecanismo democrático es la división de poderes, es decir la aceptación de que el ejercicio de los recursos, instrumentos y medios que han de poner en práctica los gobernantes elegidos, tiene que atender a la separación de dicho ejercicio en el de tres «poderes» o funciones: legislativo, ejecutivo y judicial. Ello implica que la actividad propia de cada poder ha de ser realizada respetando la distribución de las competencias funcionales establecida mediante la satisfacción de los procedimientos reconocidos y articulados por la constitución y el resto del ordenamiento. Estos procedimientos permiten garantizar tanto la independencia de acción de cada uno de los poderes, cuanto que la coordinación y el equilibrio del ejercicio de las funciones o competencias propias de los mismos.

El tercer mecanismo es el del reconocimiento, respeto, preservación y promoción de las declaraciones de derechos humanos contenidas en la constitución y el ordenamiento jurídico en su conjunto, realizados por la práctica del ejercicio de las competencias y funciones propias de los poderes con respecto a actividades ocurridas en sociedades concretas.

2.2. El acceso a información como requisito democrático

Completa lo hasta aquí expresado la consideración de que, obviamente, la democracia o la participación política no puede ser puesta en práctica efectivamente en ninguna de las facetas reseñadas sin la satisfacción de un requisito previo: que los ciudadanos estén informados o, lo que es lo mismo, tengan suficiente conocimiento sobre el objeto de su participación.

Es por ello que en la actualidad cabe decir, sintéticamente, que un sistema político democrático es aquel cuyo funcionamiento está basado en la participación consciente e informada de los ciudadanos en el ejercicio del poder político o bien indirectamente mediante la elección de sus representantes o bien directamente colaborando en la toma de decisiones políticas utilizando otros mecanismos. Esto implica reconocer que los ciudadanos pueden participar en prácticamente todas las actividades de los poderes públicos, atendiendo, además, al hecho de que el Estado de Derecho actual no es el Estado liberal del siglo XIX que li-

mitaba la acción de los organismos públicos a actuar políticamente como policía elaborando las correspondientes leyes básicas y aplicándolas mediante penas o sanciones a los infractores del orden jurídico: salvaguardando el funcionamiento del mercado, sus posibles violaciones, sino que el Estado es, a la vez, Estado social, democrático, del bienestar, de la gobernanza y, hoy, el Estado propio de la denominada sociedad del conocimiento, que tiene potestad para participar en prácticamente todas las actividades diarias, especialmente las propias de las instituciones públicas una vez están financiadas con fondos públicos.

2.3. Gobernanza

A lo dicho hasta aquí no le impide el reconocimiento que de un tiempo a esta parte se está aceptando como práctica política propia común de las competencias propias de los poderes públicos la del ejercicio de lo que se denomina gobernanza. La gobernanza está definida por el Diccionario como «Arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía».

Lo anterior implica reconocer la expansión en el ámbito público, como prácticas o usos propios de los gobernantes (incluyendo en la expresión a todos los funcionarios públicos que ponen en acción a los tres poderes), de los principios, técnicas o usos de gobierno propios del ámbito empresarial. Esto es lo mismo que decir: la puesta en acción de la eficiencia y las reglas del mercado como criterio de acción preferente de los poderes públicos.

Este estilo de acción o política no impide lo expresado en los anteriores apartados, es decir la circunstancia de que ha de ser ejercido por los poderes en forma compatible con la puesta en práctica de los principios propios del Estado de Derecho, que resumen la acción de la democracia que, por mandato legal, gobierna la acción de los poderes públicos, es decir todos aquellos asuntos sobre los que éstos son competentes según el ordenamiento propio de los Estados de Derecho en cuanto son agentes activos en la vida social y política de la sociedad del conocimiento[3]. Ello se predica especialmente de la aplicación del Derecho, realizada por los juristas, según se reconoce genéricamente, en el proceso judicial de forma compleja: atendiendo al mecanismo de la ponderación, propio de la gobernanza, más que a la aplicación «automática» de la subsunción. Es conveniente resumir a estos efectos el mensaje básico enviado por algunos de los estudiosos, filósofos del Derecho, de las decisiones judiciales a prácticos del Derecho desde un tiempo ya lejano como el constituido por los comienzos del siglo XX[4] .

Desde aquella época, justamente desde el comienzo de la obligación de los jueces de poner en ejecución el Código Civil alemán bajo su responsabilidad ante todos los casos que los

3 Se hacen propuestas a este respecto en relación al ámbito local en Estados Unidos en: Katz, E.D. (2010). Engineering the Endgame. *Michigan Law Review, 109* (3), 349-386. Me he referido a la conciliación entre gobernanza y derecho en: Galindo, F. (2007). Justicia, gobernanza y legalidad. *Seqüencia, 55*. 29-64

4 Informa sobre el estado de la cuestión de la discusión filosófico jurídica sobre estas cuestiones: Robles, G. (2010). *Teoría del Derecho*. Madrid: 3ª edición.

ciudadanos les plantearan, surgieron consideraciones críticas con respecto a la idea de que la aplicación del Derecho por los jueces estaba reducida a la realización de la subsunción del caso concreto en la Ley, como planteaban y presumían los Códigos liberales. Ehrlich, junto a los tratadistas y jueces que se integraron en el Movimiento de Derecho Libre, puso de manifiesto que el proceso de aplicación del Derecho no podía estar reducido a la subsunción una vez que la irremediable existencias de lagunas jurídicas hace que la mayor parte de las resoluciones judiciales sean creaciones «libres», de los mismos jueces, a efectos de no incurrir en la responsabilidad correspondiente por no tomar decisiones en casos, sometidos a su decisión por imperativo legal, cuyos supuestos y soluciones no coincidieran con los previstos por la Ley[5] .

A partir de estas consideraciones surgieron a lo largo del siglo XX hasta la actualidad múltiples reflexiones dirigidas a completar el proceso de aplicación judicial del Derecho con otras explicaciones. Algunas de las soluciones propuestas fueron las siguientes: el conocimiento de las concepciones y convicciones sociales (propuesta hecha por Ehrlich a través de la Sociología: el derecho vivo), la consideración de que el proceso judicial y el razonamiento jurídico están integrados por tópicos o lugares comunes que auxilian a la aplicación (Viehweg[6]), el establecimiento de sistemas normativos auxiliares a la aplicación elaborados mediante el uso de la lógica contando con la construcción de la pirámide normativa que amplía racionalmente el ámbito legal (Kelsen[7]), la propuesta del estudio de las leyes atendiendo a que se interpretan a partir de la «precomprensión» de su contenido (Esser[8], Engisch[9] y Gadamer[10]), el estudio de la aplicación judicial del Derecho atendiendo al amplio ámbito y contenido de las argumentaciones que en la misma se produce (Perelman[11], Alexy[12]), la consideración del acuerdo de legitimación social: el consenso, al que están dirigidas las leyes y la organización estatal en su totalidad (los tres poderes) en las sociedades democráticas (Habermas[13]), la consideración de que todas las actividades humanas son realizadas atendiendo a un conocimiento de la realidad producido en el contacto mantenido con la misma realidad: «autopoiéticamente» (Maturana[14]), y no por la mera elucubración o desarrollo intelectual de las propuestas científicas…

Estas y otras propuestas estaban ocupadas, resumiendo, en poner énfasis en el contexto propio de la aplicación judicial, a efectos de explicarla y darle soluciones más complejas que las que establece la subsunción o el discurrir formal sobre los textos jurídicos.

---

5 Ehrlich, E. (1966). *Die juristische Logik*. Tübingen.

6 Viehweg, T. (1974). *Topik und Jurisprudenz*. München.

7 Kelsen, H. (1949). *General Theory of Law and State*. Cambridge: 2ª edición,

8 Esser, J. (1961). *Principio y norma en la elaboración jurisprudencial del derecho privado*. Barcelona.

9 Engisch, K. (1968). *La idea de concreción en el derecho y en la ciencia jurídica actuales*. Pamplona.

10 Gadamer, H, G. (1977). *Verdad y método: fundamentos de una hermeneútica filosófica*. Salamanca.

11 Perelman, Ch. (1979). *La lógica jurídica y la nueva retórica*. Madrid.

12 Alexy, R. (1992). *Begriff und Geltung des Rechts*. Freiburg.

13 Habermas, J. (1998). *Facticidad y validez: sobre el derecho y el Estado democrático de derecho en términos de teoría del discurso*. Madrid.

14 Maturana, H. (1990). *El árbol del conocimiento: las bases biológicas del conocimiento humano.* Madrid.

3. TIC Y DEMOCRACIA

No cabe duda de que las Tecnologías de la Información y la Comunicación (TIC) e Internet facilitan la puesta en funcionamiento de los sistemas políticos democráticos. Aquí vamos a presentar tres ejemplos que lo prueban inequívocamente. Uno está referido al auxilio a la elección de los representantes políticos. Otro se refiere al acceso de los ciudadanos a los servicios públicos por medios electrónicos. El último se ocupa del apoyo al funcionamiento del poder judicial. A continuación resumimos las características básicas de los ejemplos.

El primer ejemplo tiene manifestaciones masivas en Brasil, por ejemplo. Desde la segunda mitad de los años noventa los procesos electorales destinados al nombramiento de los representantes políticos son auxiliados por el uso de las denominadas «urnas electrónicas», programas y ordenadores que facilitan que el derecho de voto con el fin de elegir a sus representantes políticos que tienen todos los ciudadanos sea ejercido por la selección por los electores de los candidatos mediante la pulsación, autorizada por los integrantes de la mesa de votación a los electores que son identificados mediante la aportación de un documento, del número correspondiente, la denominación, asignado a los candidatos a ser elegidos. El programa almacena las opciones tomadas por los electores y suma los resultados finales de la votación. De esta forma el uso de las tecnologías mejora el ejercicio del voto al dificultar la realización de prácticas corruptas electorales que en Brasil permitían los sistemas tradicionales de elección política, promoviendo con ello el uso de las TIC la ampliación y profundización de la democracia[15].

El segundo ejemplo está extendido por muchos países. Es el denominado Gobierno electrónico o, más adecuadamente, Administración electrónica[16]. Hace referencia a la provisión por medios electrónicos de acceso de los ciudadanos a los servicios públicos. Implica que los ciudadanos puedan tramitar por Internet desde sus domicilios o sus propios ordenadores instancias a las Administraciones Públicas sin necesidad de realizar desplazamientos a la sede de las Administraciones de las que se requiera la satisfacción de un derecho concreto. El proceso tiene lugar de la siguiente forma. Una vez identificado fidedignamente el solicitante mediante la utilización de una clave obtenida usando un procedimiento seguro, el ciudadano interesado puede remitir por Internet su solicitud, junto al expediente que la

15 Véase al respecto: Mezzaroba, O., Rover, A.J. (2009). A urna eletrônica: sua contribuição para o aperfeiçoamento da democracia representativa partidária brasileira. En Galindo, F., Rover A.J., (eds.), *Derecho, gobernanza y tecnologías de la información en la sociedad del conocimiento*, (63-73). Zaragoza: LEFIS Series 7, Prensas Universitarias.

16 El plan de gobierno electrónico de la Unión Europea para el período 2011-15 está regulado en: *Com-munication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The European eGovernment Action Plan 2011-2015. Harnessing ICT to promote smart, sustainable & innovative Government (2010), COM/2010/0743 final*. Recuperado el 14 de marzo de 2012 en http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:DKEY=548503:EN:NOT

justifica o fundamenta, al ordenador-programa de la Administración, la sede electrónica, cuya sección administrativa competente tiene la obligación de tramitar el expediente reconociendo lo requerido por el solicitante. El sistema tecnológico puede mejorar, por tanto, la calidad democrática de la Administración correspondiente, al incrementar la prontitud de respuesta de los servicios que la integran, potenciando de esta forma la satisfacción de los derechos de los ciudadanos[17].

El tercer ejemplo está referido al ámbito judicial y sucede en varios países. Por ejemplo[18]. Un abogado, convenientemente identificado, puede enviar a un Juzgado o Tribunal desde cualquier ordenador un documento que forme parte de un proceso en el que esté implicado un ciudadano defendido (o acusado) por el abogado, a efectos de que el trámite procesal se dé por realizado pudiéndose con ello continuar su tramitación en un periodo de tiempo menor que el que es preciso para que el procedimiento discurra por los canales establecidos para la tramitación del documento en formato papel al evitarse las dilaciones propias del funcionamiento del correo ordinario. El sistema, además, permite a todas las partes implicadas en el proceso comprobar el estado de tramitación del procedimiento, pudiéndose conocer tanto las fases del proceso satisfechas cuanto el contenido de los documentos presentados por la otra parte o las resoluciones o diligencias adoptadas por el órgano instructor o juzgador. Las TIC favorecen también en este caso la democracia una vez que el procedimiento que facilitan permite tanto acortar los tiempos precisos para el ejercicio de las labores propias del poder judicial: la resolución de conflictos, cuanto hacer más transparentes las fases de tramitación del procedimiento, permitiendo conocer por las partes implicadas en el caso el estado en el que la tramitación se encuentra, sin que por ello pierda el proceso judicial las funciones conferidas al mismo por el ordenamiento democrático.

No cabe duda de que estos procesos son ejemplos de que las TIC son efectivos instrumentos auxiliares del funcionamiento de los sistemas democráticos.

A efectos de explorar otras posibilidades discurrimos en el resto del trabajo sobre si las TIC permiten:

- auxiliar al proceso de elección de los representantes políticos, además de completar la mecánica de puesta en práctica del proceso electoral en algunos aspectos problemáticos del mismo, y
- mejorar la participación de los ciudadanos en la puesta en acción del Estado de Derecho permitiéndoles intervenir en decisiones políticas con un mayor y mejor conocimiento de la realidad política y su funcionamiento que el que tienen sin el uso de las TIC.

17 Sobre servicios administrativos en línea para ciudadanos en España véase: http://www.060.es/060/appmanager/portal/desktop/page/ciudadanosHome. Recuperado el 14 de marzo de 2012

18 Se toma como referencia el funcionamiento del sistema español LEXNET: «sistema informático de te-lecomunicaciones Lexnet para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos», regulado por el Real Decreto 84/2007, de 26 de enero. La página web del sistema LEXNET es: http://infolexnet.justicia.es/. Recuperado el 14 de marzo de 2012.

4. DEMOCRACIA E INTERNET

Ha quedado reseñado al comienzo de este trabajo que la expresión democracia se utiliza con gran frecuencia como vocablo caracterizador de Internet. Se dice que promueve la participación; que presenta a la opinión pública: a los ciudadanos, información que antes se encontraba sólo en poder de organismos gubernamentales o partidos políticos; que permite expresar a todos opiniones ante cualquier asunto que presenten en la red Gobiernos, particulares, asociaciones o empresas…

En este apartado presentamos algunos de los límites que cabe hacer a este tipo de afirmaciones. En concreto nos centramos en:

- mostrar las características básicas de los usos que se hace de Internet en estos momentos, y
- reseñar algunas de las características de la gobernanza de Internet, especialmente en lo relativo a la posibilidad de manifestar opiniones libre y secretamente.

4.1. Internet y promoción de la democracia

A efectos de considerar datos concretos nos fijamos en información referida al uso de Internet en dos ámbitos: porcentaje de casas o domicilios con acceso a Internet y porcentaje de declaraciones de usos de las aplicaciones de Internet.

4.1.1. Domicilios

No cabe negar el elevado grado de acceso a Internet que se produce en estos momentos. Acudiendo a estadísticas oficiales (EUROSTAT), estas dan cuenta de que la cifra promedio de viviendas con acceso a Internet en Europa en 2011 es del 73 por ciento de las mismas, frente al 49 por ciento de 2006. El porcentaje todavía aumenta más si se considera el número de viviendas con acceso a Internet en las que viven niños: llegaba al 84 por ciento en 2010, mientras que el promedio de viviendas con acceso a Internet en las que no viven niños alcanzaba al 65 por ciento (en 2010)[19].

4.1.2. Aplicaciones usadas

Existen también datos estadísticos sobre el tipo de las aplicaciones, programas o usos que se hace de Internet. Según dichos datos se utiliza Internet básicamente para realizar los siguientes tipos de comunicaciones:

1. correo electrónico,

19 Vease al respecto los resultados de la encuesta titulada «Households with Internet access at home»: http://epp.eurostat.ec.europa.eu/tgm/refreshTableAction.do?tab=table&plugin=1&pcode=tin00088&language=en. Recuperado el 13 de marzo de 2012.

2. envío de mensajes a programas –páginas web- que facilitan la realización de conversaciones simultáneas («chats») y publicación de noticias («blogs»), y
3. realización de llamadas telefónicas y videoconferencias[20].

Es lógico considerar que cuando nos ocupamos de democracia sólo las comunicaciones referidas en segundo lugar: el envío de mensajes a programas o páginas web, pueden ser tomadas como referencia para discurrir sobre un posible ejercicio de la democracia utilizando Internet. Recuérdese que, tal y como vimos en el primer apartado (2.1), democracia es lo mismo que emisión de opiniones con relevancia pública o «participación de los ciudadanos en el ejercicio del poder político o bien indirectamente mediante la elección de sus representantes o bien directamente colaborando en la toma de decisiones políticas utilizando otros mecanismos». Los otros usos, tanto el intercambio de correos electrónicos, como las conversaciones telefónicas o las videoconferencias, están referidos a comunicaciones privadas habidas entre los interlocutores que los utilizan.

Considerando los datos estadísticos, es interesante comprobar, contemplando las cifras recopiladas sobre uso de Internet en Europa[21], que hay una diferencia sustancial en el porcentaje de usuarios que en 2010 utilizaron Internet para realizar «chats», enviar «blogs» y participar en actividades de redes sociales: 75 (entre 16 y 24 años), 33 (entre 25 y 54) y 7 (entre 55 y 74); el promedio de uso de estas herramientas fue el 32 por ciento de la totalidad de los usuarios. La diferencia es más destacable si se tiene en cuenta que frente a estos datos el promedio general de individuos que en Europa utilizaron en 2010 Internet para enviar y recibir mensajes por correo electrónico en 2010 fue mucho más superior: prácticamente el doble, el 61 por ciento[22].

4.1.3. Conclusiones sobre el uso de Internet y democracia

Los datos hasta aquí expuestos nos permiten concluir lo siguiente.

Si bien es indudable la fuerte expansión alcanzada por Internet, el promedio del acceso a la red es del 73 por ciento de los domicilios europeos, ello no permite, hipotéticamente, por ejemplo, la aprobación de una norma de ámbito europeo que establezca la obligación de elegir a los representantes políticos usando las TIC: desde los propios ordenadores. Para que esta norma pudiera entrar en vigor debería ser posible un acceso del cien por cien de la población, lo que no se produce en la actualidad.

---

20 El promedio europeo de realización de llamadas telefónicas y videoconferencias por internet por personas era muy bajo: 10 por ciento en 2007 cuando se realizó la encuesta. Ver: «Internet activities – Individuals: Internet use: telephoning, videoconferencing»: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ci_ac_i& lang=en . Recuperado el 14 de marzo de 2012.

21 «Individuals using the Internet for posting messages to social media sites or instant messaging. Posting messages to chat sites, social networking sites, blogs, newsgroups or online discussion fora or use of instant messaging»: http://epp.eurostat.ec.europa.eu/tgm/refreshTableAction.do?tab=table&plugin=0&pcode=tin00084& language=en . Recuperado el 13 de marzo de 2012.

22 «Internet use and activities: sending/receiving emails» http://appsso.eurostat.ec.europa.eu/nui/show.do? dataset=isoc_ci_ac_i&lang=en . Recuperado el 13 de marzo de 2012.

La expansión de la democracia tampoco es viable absolutamente en estos momentos si tenemos en cuenta las características de los usos de Internet. Como hemos visto tan sólo el sector más joven de la población: el comprendido entre los 16 y los 24 años, utiliza mayoritariamente sistemas que permiten expresar opiniones (el 75 por ciento de ellos atendiendo a las cifras generales europeas) mientras que los otros dos sectores entre 25 y 54 y entre 55 y 74 los usan en escasa medida (33 y 7 por ciento respectivamente).

4.2. La gobernanza de Internet

Existe otro problema de mayor entidad que el del reducido número de usuarios que acostumbra a emitir opiniones usando la red que acabamos de señalar como límite para la expansión de la democracia por Internet. El problema de mayor envergadura está ligado a las características del funcionamiento de Internet y su regulación, que impiden garantizar el secreto de las opiniones emitidas, principio que, entre otros, requiere la puesta en acción de los procesos democráticos. A este problema lo identificamos como la gobernanza de Internet.

Con gobernanza de Internet nos referimos a las reglas básicas de funcionamiento del sistema, que, más allá del uso de las tecnologías, vienen a ser, con algunas moderaciones, las mismas que las del mercado o la obtención de beneficios.

En efecto. La utilización de Internet requiere, indefectiblemente, al ciudadano el pago de su uso: básicamente a la compañía de telecomunicaciones que garantiza la comunicación y al proveedor de servicios de acceso a Internet que permite la «navegación», también a los que ofertan servicios «accesibles» a través de la red. El último pago se hace de una forma indirecta: o bien al abonar los precios de los bienes adquiridos una vez que en dicho precio están repercutidos los costes de comercialización y envío del producto hechos por el vendedor utilizando Internet, o bien, en el caso del acceso a servicios públicos, al pagar los impuestos y tasas al Estado, una vez que parte de ellos sirve para satisfacer el coste de los servicios que son accesibles y tramitados por Internet.

A lo anterior ha de añadirse otra faceta o dimensión, si tomamos en consideración la hipótesis de la utilización de Internet como canal para ejercer la democracia en el proceso de elección de gobernantes o mediante la emisión de opiniones en referéndum sobre un tema sometido a decisión de los ciudadanos por las instituciones públicas. La nueva dimensión procede de la circunstancia de que si bien, como ya veíamos en los ejemplos mencionados más arriba (3) referidos al acceso a los servicios de las Administraciones públicas o a la tramitación de expedientes judiciales, el ejercicio de dicho acceso requiere la inequívoca identificación de quien emite su opinión, tal y como sucede en la solicitud de servicios públicos o en la actuación en la Administración de justicia: ha de saberse quién ejerce su derecho y que lo hace en un momento concreto, mientras que la actuación de la democracia por medio de las elecciones, en cambio, requiere algo más: garantizar y preservar el secreto de las opiniones emitidas a efectos de que estas sean hechas en libertad (las exigencias del voto son: sufragio universal, libre, igual, directo y secreto). Y aquí es dónde la relación entre democracia e Internet tiene tantas dificultades que cabe decir, incluso, que por el momento esa relación no es posible ni siquiera contando con recursos tecnológicos como enfatizamos a continuación.

Tanto la procuración electrónica de servicios públicos como la remisión de documentos a instancias judiciales requiere garantizar la autenticidad del remitente, la del proceso de comunicación o el envío de los documentos: que no sea interceptado, y la de que el contenido de lo enviado sea lo efectivamente remitido por el emisor, lo que sucede mediante la utilización de los requisitos técnicos expuesta resumidamente más arriba, sin que dichos procedimientos requieran mantener permanentemente el secreto del contenido del comunicado. Es más: en la tramitación de procedimientos administrativos y judiciales es preciso, básicamente, poder evidenciar a lo largo de todo el procedimiento que el contenido de los documentos comunicados es el refrendado por el remitente.

El requisito fundamental para garantizar el funcionamiento del proceso de emisión de una opción u opinión política, en cambio, es el de la preservación permanente del secreto de la opción u opinión del responsable, de otra forma los electores u opinantes no pueden contar con suficiente libertad como para emitir su voto u opción, otro principio básico democrático. El problema reside en que si bien la identificación fidedigna es posible, como ocurre en los ejemplos mencionados en el apartado (3), mediante la utilización de sistemas TIC de identificación, de coste mayor o menor, la garantía de la preservación del secreto y de la emisión libre de las opiniones no es posible ponerla en práctica sino, a lo sumo, mediante la utilización de mecanismos como el cifrado de clave pública de confidencialidad, de uso general no autorizado en estos momentos por razones de seguridad[23].

Es decir: en el caso de las elecciones por Internet el principio de seguridad pública establece fuertes límites al principio de mercado o de las reglas de gobernanza que rige el funcionamiento propio de Internet, y que es el que delimita en estos momentos, básicamente, la práctica relativa a la libre expresión de ideas que se manifiesta entre los usuarios de Internet mediante el uso de instrumentos de comunicación como el acceso a las redes sociales, el envío de noticias a los «blogs» o el intercambio de mensajes utilizando sistemas de correo electrónico, comunicación telefónica o videoconferencia.

5. USO DE INSTRUMENTOS TÉCNICOS Y BRECHA DIGITAL

Es conveniente reconsiderar la información que suministran los datos estadísticos para tener una mayor conciencia sobre las posibilidades e implicaciones que tiene un hipotético

23 Sobre los pros y contras de las «elecciones electrónicas» ver: Alvarez, R.M. y Hall, T. E. (2010). *Electronic Elections: The Perils and Promises of Digital Democracy*. Princeton y Oxford. Se establecen indicaciones por el Consejo de Europa sobre los requisitos para poner en funcionamiento a la democracia electrónica en forma respetuosa con los principios democráticos en la Recommendation CM/Rec(2009)1 of the Committee of Ministers to member states on electronic democracy (e-democracy) (Adopted by the Committee of Ministers on 18 February 2009 at the 1049th meeting of the Ministers' Deputies), ver al respecto: Council of Europe. Ad Hoc Committee on E-democracy, Council of Europe. Committee of Ministers (2009). *Electronic democracy («e-democracy») Recommendation CM/Rec(2009)1 and explanatory memorandum*. Strasbourg.

intento de realizar un ejercicio de la democracia, entendida como ejercicio del sufragio político, utilizando las herramientas y mecanismos que proporciona Internet.

En el apartado anterior hemos observado que no es posible realizar elecciones políticas por medio de Internet por varias razones, en este apartado vamos a matizar todavía más el alcance de los argumentos mostrando que cuando pasamos de considerar los promedios estadísticos generales referidos a un amplio espectro de la población a atender a los relativos a determinados países las cifras tienen contenidos, y significación, distintos.

Fijémonos en las cifras referidas al porcentaje de viviendas con acceso a Internet. Decíamos que el acceso promedio en Europa era alto: el 73 por ciento de las casas lo tenía en 2011, y 84 %, ya en 2010, era el promedio de las casas con niños. Las cifras alcanzan distinto cariz si nos fijamos en España cuyos porcentajes son, respectivamente, 64 y 73, Alemania, 83 y 97 o Rumanía, 47 y 50, por ejemplo[24]. El matiz todavía es más importante si nos fijamos en Suramérica. En Brasil, en 2010, sólo el 27 por ciento de las casas contaba con acceso a Internet, siendo el mismo número promedio el del 31 por ciento en las viviendas situadas en ámbito urbano y el 6% en las viviendas situadas en ámbito rural[25].

Estos datos dan cuenta de la existencia efectiva de la denominada brecha digital y de cómo la reflexión sobre la posibilidad de votar a través de Internet es un discurso estrecho: de limitado alcance social inmediato, necesita ser completado. Pensemos en que una hipotética puesta en práctica inmediata que requiriera su uso obligatorio en un país implicaría privar del derecho de voto a un ingente número de personas.

6. ACCESO A INFORMACIÓN

Expresábamos al comienzo de este trabajo (2.2) que un requisito fundamental para el ejercicio de la democracia es contar con información suficiente para decidir. Ello es coherente con el hecho de que sin información no es posible tomar decisión alguna[26]. Si esto es así en las actividades propias: en el ejercicio de la libertad o del principio de autonomía de

24 Ver: los resultados de la encuesta titulada «Households with Internet access at home»: http://epp.eurostat.ec.europa.eu/tgm/refreshTableAction.do?tab=table&plugin=1&pcode=tin00088&language=en . Recuperado el 14 de marzo de 2012.

25 Ver: «PROPORÇÃO DE DOMICÍLIOS COM ACESSO À INTERNET» http://www.cetic.br/usuarios/tic/2010-total-brasil/rel-geral-04.htm . Recuperado el 14 de marzo de 2012). Los datos son recopilados por el brasileño «Centro de Estudos sobre as Tecnologias da Informação e da Comunicação» (CETIC.br)

26 Sin establecer contactos con el exterior. Ver al respecto Maturana, H. (2006). Self-consciousness: How? When? Where?. *Constructivist Foundations, 1* (3), 91-102. En este artículo se muestra el origen de la auto-consciencia, mostrándola como un suceder que ocurre en el «lenguajear», y no confundiendo los dominios en los cuales ocurre el vivir, ni reduciéndolos. Para esto se basa en los fundamentos biológico-culturales de lo humano, buscando siempre el mecanismo estructural-operacional que da origen al fenómeno por el cual se pregunta sin introducir nociones semánticas. El autor también reflexiona sobre las consecuencias y alcances de este mirar, esto es, que la autoconsciencia no ocurra en

la voluntad, la misma o mayor relevancia tiene en el ámbito de acción de los hombres referido a las actividades que implican a otros hombres. Especialmente en la acción política y el ejercicio democrático de la libre elección de los representantes políticos: no se puede elegir sin conocer previamente las opciones sobre las que cabe optar.

E Internet proporciona, sin duda, acceso a información. Ofrece una información que antes, sin la red, no estaba al alcance de los ciudadanos. La información quedaba, a lo sumo, recogida en documentos: estudios, informes, artículos científicos y de opinión, libros y noticias suministrada por los medios de publicación, opinión e información: periódicos, revistas y otros medios (televisión y radio fundamentalmente). Otra parte de la información y especialmente la referida a las actividades del Estado quedaba fuera de los círculos de opinión. Con gran frecuencia se consideraba secreta: estaba a disposición únicamente de las instituciones estatales.

La información necesaria para elegir democráticamente es la referida a las actividades de los representantes políticos, cuya expresión se manifiesta en la acción propia de las instituciones en las que los mismos las realizan. Son las actividades de los poderes legislativo, ejecutivo y judicial. Están recogidas en leyes, normas, reglamentaciones, sentencias y, ahora, también en páginas web en las que se presenta tanto el contenido de las regulaciones cuanto que informaciones sobre las características y resultados de las actividades desenvueltas y los servicios públicos ofertados por cada institución.

La información relativa al contenido de las regulaciones es la misma, sobre formato digital, que la que se hacía pública en papel. La principal diferencia resulta del grado de expansión de la información digital: es mayor que la que tiene la recogida en formato papel. La información sobre las instituciones, sus actividades y servicios, es de diferente entidad: tradicionalmente no era accesible, no existía o a lo sumo encontraba algún eco en los medios de comunicación. En la mayor parte de las ocasiones estaba expresada en el contenido de los propios textos jurídicos o regulaciones. En la actualidad esta información es generada por la propia institución, que puede ofrecer sus servicios a los ciudadanos a través de Internet, como recogíamos más arriba (apartado 3).

Esta información precisa ser expuesta, publicitada y recopilada de forma ordenada y suficientemente clara si se quiere que los ciudadanos puedan acceder a la misma, utilizar los servicios públicos y realizar el control democrático de la misma que compete a los ciudadanos. Paso previo es el establecimiento de algunas indicaciones para efectuar adecuadamente esta recopilación, atendiendo tanto al contenido de las prácticas desarrolladas como a lo que prescriben las reglas de la democracia encaminadas a potenciar la participación de los ciudadanos en el poder político. En España no se ha promulgado una Ley de transparencia y acceso a la información pública que es la que debe dar indicaciones generales sobre la información a publicar. La única regulación existente, por ahora, es la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del

---

el cerebro y que no sea una entidad física sino que está ocurriendo como una configuración de sentires (sensorialidades) en un presente en continuo cambio.

sector público estatal y el Real Decreto 1495/2011 que desarrolla la Ley[27]. Esta normativa es insuficiente al no estar desarrollado el marco general el gobierno y las instituciones públicas no están obligadas a facilitar a los ciudadanos la información necesaria para tomar decisiones importantes en el ámbito personal, profesional y político. Es por ello que hasta ahora lo que existen son iniciativas que tienen por objeto hacer llegar a los ciudadanos información pública: «open data», que se encuentra en Internet[28].

La más mínima observación sobre la información recopilada por este tipo de iniciativas[29] da cuenta de que responde a fines u objetivos dispares: ofertar la información a elaboradores de estudios, disponer acceso seguro a servicios públicos, mostrar el alcance de las iniciativas administrativas propias de la entidad administrativa responsable de la página o sitio web, señalar los avances de la técnica, poner en funcionamiento el principio legal de transparencia de las actividades gubernamentales, mostrar el grado de eficiencia de políticas de gobernanza, generar actividades a desarrollar por empresas y con ello crear empleo… Todo lo cual trae como consecuencia la existencia de numerosa información en Internet que está situada, todavía, en forma escasamente accesible al ciudadano, una vez que éste no cuenta con suficientes conocimientos ni recursos como para poder acceder a la información ni, una vez accedida, comprenderla. Ello, por tanto, no se debe únicamente al limitado porcentaje de personas que acceden a la red del que se daba cuenta en las estadísticas recogidas en apartados anteriores, la brecha digital, sino al hecho de que la información está colocada con gran frecuencia en lenguaje propio de profesionales expertos en contabilidad, por ejemplo, pero no en lenguaje comprensible por los ciudadanos.

Es por ello que de un tiempo a esta parte se producen otras iniciativas que tienen el objetivo de formar a profesionales y promover la participación ciudadana en forma activa en el ejercicio de sus derechos democráticos, haciendo accesible mediante Internet a los ciudadanos el mismo funcionamiento y actividades de las Administraciones públicas y de los diferentes poderes públicos.

En este marco de acción se encuentran las investigaciones y desarrollos que desde 2003 se realizan por el Observatorio Internacional de Gobierno electrónico.

---

27 Se puede acceder a la Ley en http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-19814. Al Real Decreto en: http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-17560 . Ponen en práctica la Directiva europea sobre transparencia: Directiva 2003/98/CE del Parlamento Europeo y del Consejo de 17 de noviembre de 2003 relativa a la reutilización de la información del sector público. http://eurlex.europa.eu/LexUriServ/LexUriServ .do?uri=CELEX:32003L0098:ES:HTML

28 Elaborados por el Gobierno del País Vasco: http://opendata.euskadi.net/w79-home/es. Sobre actividades administrativas del Gobierno del Reino Unido: http://data.gov.uk/. La Fundación sobre datos abiertos, organización no lucrativa, promueve el uso de datos estadísticos: http://www.opendatafoundation.org. Las páginas web han sido accedidas el 15 de marzo de 2012.

29 Vease la información contenida en iniciativas gubernamentales españolas sobre «open data» como APORTA (http://www.aporta.es/web/guest/news.consulok, consultado el 14 de marzo de 2012) y Datos.gob.es (http://datos.gob.es/datos/, consultado el 14 de marzo de 2012).

El objetivo fundamental del Observatorio EGOBS (Electronic Government Observatory) es el estudio independiente de las características de las realizaciones que en materia de Gobierno electrónico tienen lugar en distintos países.

Los trabajos realizados ponen especial énfasis en la comprobación referida a si la prestación se realiza con respeto a las normas, procedimientos y principios recogidos en las leyes, incluido el derecho a la participación en dichas actividades de ciudadanos, empresas e instituciones y, especialmente, si se satisface en su puesta en práctica las regulaciones sobre protección de datos y seguridad de las comunicaciones electrónicas.

EGOBS (www.egobs.org)[30] es una iniciativa surgida de la red temática Gobierno Electrónico coordinada por la Universidad de Zaragoza (España) y en cuyas actividades participan desde 2003 las Universidades de Burgos y Valladolid (España), de Münster (Alemania) y la Queen's University de Belfast (Reino Unido), por parte europea. Los miembros americanos son la Universidad Nacional de la Plata (Argentina), la Diego Portales de Santiago de Chile, la de la Habana (Cuba) y la de la República de Montevideo (Uruguay). El Observatorio es parte de la Red Jurídica para la Sociedad de la Información LEFIS (Legal Framework for the Information Society)[31].

Desde el 1 de enero de 2009 el Observatorio cuenta con infraestructura personal y material para el desarrollo de sus actividades en Iberoamérica. En concreto en la Universidad Federal de Santa Catalina (Brasil)[32].

Las actividades de observación de EGOBS han estado centradas en aplicar, con fines docentes e investigadores, una metodología desarrollada para estudiar páginas web, confeccionadas e implementadas por Administraciones públicas, utilizando criterios de análisis que permiten conocer y presentar públicamente las características de las propias páginas, sus contenidos y el de las ofertas de servicios que realizan las Administraciones que las han confeccionado y mantienen[33].

---

30 La página ha tenido 215.387 visitas entre el 1.1.2007 y el 15.3.2012. Los visitantes procedían de 147 países/regiones. Los diez primeros países por número de visitas (de mayor a menor) son: Estados Unidos, China, Chile, España, Méjico, Uruguay, Federación Rusa, Argentina, Venezuela y Perú. Los informes sobre visitas han sido elaborado teniendo en cuenta la información que recopilar el programa URCHIN de Google.

31 La página ha tenido 1.071.805 visitas entre el 1.1.2007 y el 15.3.2012. Los visitantes procedían de 204 países/regiones. Los diez primeros países por número de visitas (de mayor a menor) son: Estados Unidos, China, España, Japón, Letonia, Alemania, Federación Rusa, Reino Unido, Francia y Brasil. Los informes sobre visitas han sido elaborado teniendo en cuenta la información que recopilar el programa URCHIN de Google.

32 http://www.egov.ufsc.br/portal/. La página ha sido accedida el 15 de marzo de 2012. La página ha tenido 1.092.775 visitas entre el 1.1.2011 y el 15.3.2012. Los visitantes procedían de 174 países/regiones. Los diez primeros países por número de visitas (de mayor a menor) son: Brasil. Estados Unidos, China, Portugal, Reino Unido, Japón, Francia, España, Alemania y Mozambique. Los informes sobre visitas han sido elaborado teniendo en cuenta la información que recopilar el programa URCHIN de Google.

33 La métrica LEFIS. Ver su contenido en: http://www.egobs.unizar.es/index.php?option=com_content&%2520task=view&id=14&Itemid=27. La página ha sido accedida el 15 de marzo de 2012.

La metodología se ha venido aplicando desde el año 2005 a páginas web desarrolladas por instituciones públicas en Chile, Uruguay, España y Brasil, fundamentalmente. Los resultados de los análisis están expuestos en Internet[34].

A partir de 2009 EGOBS realiza en la misma línea otro tipo de análisis destinado a presentar en Internet a ciudadanos en forma clara la localización geográfica de instituciones públicas que realizan distintas actividades. Este tipo de información se refiere básicamente a instituciones brasileñas. Los estudios se expresan en forma de páginas web que contienen mapas de Brasil en los que se recoge la localización de instituciones y actividades realizadas por las mismas en relación a materias concretas[35].

La lista de materias en forma de temas generales en la actualidad es la siguiente: medio ambiente; cultura y educación pública; democracia, convergencia e inclusión digital; hacienda pública, poder judicial, ministerio público, modelos y proyectos de gobierno electrónico, salud pública y seguridad pública. En relación a cada tema se presentan varios mapas de ámbito federal o estatal, en los cuales, por ejemplo, se localiza la situación de instituciones, centros de estudio, actividades realizadas, distribución de recursos públicos con respecto a proyectos concretos, sitios web analizados siguiendo la metodología LEFIS.

Los mapas son resultados de investigaciones realizadas bajo la responsabilidad de investigadores concretos que elaboran trabajos o artículos sobre la respectiva materia. Pretenden crear discusión, a la vez que, fundamentalmente, ilustrar sobre las materias estudiadas a ciudadanos que no tengan formación especializada sino simplemente interés por conocer cuestiones concretas a efectos de crear opinión política. En este sentido son instrumentos tecnológicos que fomentan la democracia.

7. CONCLUSIÓN

Las expuestas en este trabajo son diferentes formas, concretas, de crear democracia «electrónica» mediante Internet y por ello son distintas posibilidades de incrementar la democracia. Las posibilidades muestran que aunque la democracia en Internet siempre estará limitada por el funcionamiento inevitablemente «interesado» de la gobernanza de Internet, hay margen para incrementarla, entendida ésta como participación ciudadana en el conocimiento de las actividades públicas propiciando al mismo tiempo la inclusión digital utilizando los recursos que contiene Internet.

34 Ver: http://www.egobs.unizar.es/index.php?option=com_content&task=view&id=21&Itemid=64 y http:// www.egobs.unizar.es/index.php?option=com_content&task=view&id=26&Itemid=69. Las páginas han sido accedidas el 15 de marzo de 2012.

35 Ver los mapas en: http://egov.ufsc.br/portal/mapa#mapabove. La página ha sido accedida el 15 de marzo de 2012.

8. BIBLIOGRAFIA

Alexy, R. (1992). *Begriff und Geltung des Rechts*. Freiburg.

Alvarez, R.M. y Hall, T. E. (2010). *Electronic Elections: The Perils and Promises of Digital Democracy*. Princeton y Oxford

Carbonell, M. (2008). Constitution's functionality and social rights: outline of some problems. *Estudios Constitucionales, 6* (2), 43-71.

Council of Europe. Ad Hoc Committee on E-democracy, Council of Europe. Committee of Ministers (2009). *Electronic democracy («e-democracy») Recommendation CM/Rec(2009)1 and explanatory memorandum.* Strasbourg.

Ehrlich, E. (1966). *Die juristische Logik*. Tübingen.

Engisch, K. (1968). *La idea de concreción en el derecho y en la ciencia jurídica actuales*. Pamplona.

Esser, J. (1961). *Principio y norma en la elaboración jurisprudencial del derecho* privado. Barcelona.

Gadamer, H, G. (1977). *Verdad y método: fundamentos de una hermeneútica filosófica*. Salamanca.

Galindo, F. (2007). Justicia, gobernanza y legalidad. *Seqûencia, 55*. 29-6.

Habermas, J. (1998). *Facticidad y validez: sobre el derecho y el Estado democrático de derecho en términos de teoría del discurso*. Madrid.

Katz, E.D. (2010). Engineering the Endgame. *Michigan Law Review, 109* (3), 349-386.

Kelsen, H. (1949). *General Theory of Law and State*. Cambridge: 2ª edición.

Maturana, H. (1990). *El árbol del conocimiento: las bases biológicas del conocimiento humano.* Madrid.

Maturana, H. (2006). Self-consciousness: How? When? Where?. *Constructivist Foundations, 1* (3), 91-102.

Mezzaroba, O., Rover, A.J. (2009). A urna eletrônica: sua contribuição para o aperfeiçoamento da democracia representativa partidária brasileira. En Galindo, F., Rover A.J., (eds.), *Derecho, gobernanza y tecnologías de la información en la sociedad del conocimiento*, (63-73). Zaragoza: LEFIS Series 7, Prensas Universitarias.

Perelman, Ch. (1979). *La lógica jurídica y la nueva retórica*. Madrid.

Robles, G. (2010). *Teoría del Derecho*. Madrid: 3ª edición.

Viehweg, T. (1974). *Topik und Jurisprudenz*. München.

INTERNET CO-REGULATION AND CONSTITUTIONALISM: TOWARDS EUROPEAN JUDICIAL REVIEW

Christopher T. Marsden
Essex School of Law

ABSTRACT: This article analyzes co-regulation, by defining and exploring its recent institutional history in the Internet environment. It then assesses the legal definitions and taxonomies of co-regulation before constructing a twelve-point scale of self- and co-regulation. Co-regulation has enriched conceptions of 'soft law' or 'governance' in the literature in the past ten years, but like those umbrella terms, refers to forms of hybrid regulation that do not meet the administrative and statute-based legitimacy of regulation, yet clearly perform some elements of public policy more than self-regulation, which is defined by the absence of formal roles for the nation-state or European law. Recent European case law has seen a long overdue emphasis placed on human rights in judicial review of co-regulatory arrangements. The article concludes that without regulation responsive to both market and constitutional protection of fundamental rights, Internet regulatory measures cannot be self-sustaining.

KEYWORDS: Internet law, co-regulation, self-regulation, judicial review, human rights.

1. INTRODUCTION: EXAMINING THE ORIGINS OF CO-REGULATION

This article analyzes co-regulation, by defining and exploring its recent institutional history together with that of Internet self-regulation. It then assesses the legal definitions and taxonomies of co-regulation before constructing a twelve-point scale of self- and co-regulation. It explores the possibility for judicial review of co-regulatory arrangements, recent case law that concerns human rights and Internet co-regulation, and argues for the 'constitutionalisation' of co-regulation.

The term 'co-regulation' encompasses a range of different regulatory phenomena, which have in common the fact that the regulatory regime is made up of a complex interaction of general legislation and a self-regulatory body. Co-regulation is often identified with the rise of the 'new governance' in the 1990s. Recent European case law has seen a long overdue emphasis placed on human rights in judicial review of co-regulatory arrangements. Co-regulation constitutes multiple stakeholders, and this inclusiveness results in greater legitimacy claims. The state, and stakeholder groups including consumers, are stated to explicitly form part of the institutional setting for regulation. However, direct government involvement including sanctioning powers may result in the gains of reflexive regulation – speed of response, dynamism, international cooperation – being compromised. The growing gulf between states' preference for regulatory and self-regulatory solutions, and citizens' preferences for greater control if not ownership of vital regulated industries, has led to a crisis of constitutional legitimacy.

It is a commonplace to state that the modern state has faced twin demands for less, and better designed, regulation[1]. This argued for an industry-led response to the complexity inherent in many modern regulated industries, notably the complexity associated with globalisation of businesses and the rise and ubiquity of modern (notably information and communications) technologies. The trend towards co-regulation suggests a rolling back from earlier self-regulation[2], with an involvement of public interest groups as well as government, to create greater representation in the co-regulatory bodies and therefore (it is hoped) greater transparency, internal due process and respect for fundamental rights. However, wider re-regulatory optimism may be misplaced[3], as banking reform has been far more minimal than predicted at the depth of the crisis in early 2009[4]. Responsive regulation describes a more complex dynamic interaction of state and market[5], a break with more stable previous arrangements[6]. This applies to other globalising phenomena than the Internet, for instance financial and environmental law[7], where negative externalities are highlighted for public concern[8].

The Internet developer community has cherished self-regulation based on the Codes of Conduct[9] and Terms of Use that early Internet users employed in the scientific institutions

---

1 Baldwin, R., Hood, C. And Scott, C. eds. (1998) Socio-Legal Reader on Regulation, Oxford University Press at p.3 explain that «At its simplest, regulation refers to the promulgation of an authoritative set of rules, accompanied by some mechanism, typically a public agency, for monitoring and promoting compliance with these rules.»

2 Theories of network governance emerged from the study of the firm in organisational theory, see for instance Williamson, O.E. (1975) Markets and hierarchies: Analysis and antitrust implications, New York: Free Press; Williamson, O.E. (1985) The economic institutions of capitalism: Firms, markets and relational contracting, New York: Free Press; Williamson, O. E. (1994) Transaction cost economics and organization theory, pp.77-107in N. J. Smelser & R. Swedberg (Eds.), The handbook of economic sociology, Princeton University Press.

3 Ayres, Ian and John Braithwaite (1992) Responsive Regulation: Transcending the Deregulation Debate, Oxford University Press at p. 4

4 Davies, H. (2010) Don't bank on global reform, Prospect 25th August 2010, Issue 174, at http://www.prospectmagazine.co.uk/2010/08/dont-bank-on-global-reform/

5 Teubner G. (1986) The Transformation of Law in the Welfare State, in Teubner, G. (ed.) Dilemmas of Law in the Welfare State, Berlin: W. de Gruyter, at p.8.

6 See Baldwin R. and Black J. (2010) Really Responsive Risk-Based Regulation, Law & Policy, Vol. 32 Issue 2, pp.181-213; Black, J. (2010) Managing the Financial Crisis – The Constitutional Dimension, LSE Legal Studies Working Paper No. 12/2010.

7 See for instance Gaines, Sanford E. and Cliona Kimber (2001) Redirecting Self-Regulation, Env. Law 13, p.157

8 Gunningham, N. and Grabosky, P. (1998) Smart Regulation: Designing Environmental Policy, Oxford University Press. Gunningham N., Rees J (1997) Industry Self-regulation: An Institutional Perspective, Law & Policy 19(4). Abbott K, Snidal D. (2004) Hard and soft law in international governance, International Organization 54, pp.421-422.

9 See Helin, S., & Sandström, J. (2007) An inquiry into the study of corporate codes of ethics, Journal of Business Ethics 75, pp.253–271. Higgs-Kleyn, N., & Kapelianis, D. (1999) The role of profes-

that first developed the protocols and social standards[10]. Governments have broadly accepted that a more flexible and innovation-friendly model of regulation is required, particularly in view of the rapid growth, complex inter-relationships and dynamic changes taking place in Internet and games development. This amounted to an illusory «article of faith» for the libertarian Internet users at the start of commercial Internet use[11]. The application of criminal law in specific European cases has resulted in unintended consequences and content provider losses: consider, for instance, the 1998 German conviction of former Compuserve general manager Felix Somm[12], or the *LICRA v. Yahoo!* case[13]. There cannot be a 'no regulation' option without reference to national law. Governments adopted self-regulation as a pragmatic policy, using both hard law and much softer forms of regulation[14].

Spar explained[15] that the circle of communications development turns from prophets to pirates to pioneers to politics. The prophet in this case could be seen as John Perry Barlow, the pirate as any number of cyber-criminals in the late 1990s or Napster, the pioneers as early commercial ISPs, and the politics as the constitutional law examined in *ACLU v. Reno*[16]. She explains from her case studies of radio, satellite television and the telegraph that the noteworthy feature is that anarchy gives way to control and order[17]. The dynamism of the self-regulatory

---

sional codes in regulating ethical conduct, Journal of Business Ethics, 19, 363–374. Vrielink, Mirjan Oude, Cor van Montfort, Meike Bokhorst (2010) Codes as hybrid regulation, ECPR Standing Group on Regulatory Governance, June 17-19 2010, Dublin. Abbott K, Snidal D (2009) The Governance Triangle: Regulatory Standards Institutions and the Shadow of the State (Ch. 2) in Mattli W, Woods N (eds) The Politics of Global Regulation, Princeton University Press, pp.44-88.

10 Price and Verhulst (2000) In search of the self; Price, M. (1995) Television, The Public Sphere and National Identity, Oxford University Press

11 See Goldsmith, Jack and Wu, Tim (2006) Who controls the Internet? Illusions of a Borderless World. Oxford: Oxford University Press.

12 Bender, G. (1998) Bavaria v. Felix Somm: The Pornography Conviction of the Former CompuServe Manager', Int.J. Communications L. Pol. at: http://www.digital-law.net/IJCLP/1_1998/ijclp_webdoc_14_1_1998.html

13 Reidenberg Joel R. (2001) The Yahoo! Case and the International Democratization of the Internet, Fordham University School of Law Research Paper 11 At http://papers.ssrn.com/paper.taf?abstract_id=267148.

14 Lemley, Mark A. (2006) Terms of Use, 91 Minnesota Law Review p.459; Senden, L. (2005) Soft Law, Self-Regulation and Co-Regulation In European Law: Where Do They Meet? Electronic Journal of Comparative Law, vol. 9.1 at http://www.ejcl.org/91/abs91-3.html; Cosma, H. & Whish, R. (2003) Soft Law in the Field of EU Competition Policy, European Business Law Review, Vol. 14,. Pt. 1 pp.25-56; Hodson, Dermot and Imelda Maher (2004) Soft law and sanctions: economic policy coordination and reform of the Stability and Growth Pact, Journal of European Public Policy, Volume 11 Issue 5 pp.798–813

15 Spar, Debora (2001) Pirates, Prophets and Pioneers. Business and Politics. Along The Technological Frontier, London: Random House.

16 American Civil Liberties Union v. Reno (1997) 21 U.S. 844 of June 27 No. 96-511.

17 Spar, Debora (2001) When the anarchy has to stop, 15 October, The New Statesman, at http://www.newstatesman.com/200110150021

Internet is more adaptable than earlier technologies of radio, television, and the telegraph – not least because the medium itself can be used in a distributed networked governance structure[18].

Human rights can be maintained using market-based solutions, but there are bright lines of human rights protection by national constitutions and international instruments that should not be traded for economic benefit. Such rights are backed by constitutions from the US and French Bills of Rights forwards to the new European Charter of Fundamental Rights[19]. The Internet environment is a powerful technology for society and individuals to express their rights, as well as an environment in which such rights can be abused and curtailed due to legal, economic, technological, security and other incentives for powerful actors. Constitutional courts, notably the Court of Justice of the European Union (CJEU), are now grappling with the market/rights balance.

2. CO-REGULATION DEFINED

Co-regulation is a relatively novel phenomenon, given that state regulation and self-regulation are as old as markets[20]. Kleinstuber explained «If the State and the private regulators co-operate in joint institutions, this is called co-regulation. If this type of self-regulation is structured by the State but the State is not involved the appropriate term is regulated self-regulation.»[21] This follows the nomenclature used by Hoffman-Riem in his classic study of broadcasting[22]. It has been expanded on by Latzer[23] who further finessed the distinctions between different self-regulatory bodies' establishment and development[24].

---

18 Samuelson, Pamela (1999) A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy, 87 Calif. L. Rev. p.751

19 See Peers, S. and A. Ward Eds. (2004) The EU Charter of Fundamental Rights: Politics, Law and Policy, Oxford: Hart.

20 One could argue that the statutory monopolies granted by Royal Charter under Queen Elizabeth II in the sixteenth century were examples of co-regulation, with East India Company and other trading interests granted wide powers to self-regulate under an authorizing statute. See Imperial Gazetteer of India (1908) The Indian Empire vol. II, Historical, Oxford: Clarendon Press.

21 Kleinstuber, W. (2004) The Internet between Regulation and Governance, pp61-100 in Organisation for Security and Co-operation in Europe, The Media Freedom Internet Cookbook.

22 Hoffmann-Riem, Wolfgang (2001) Modernisierung in Recht und Kultur, Frankfurt: Suhrkamp

23 See Latzer, Michael, Just, Natascha, Saurwein, Florian, Slominski, Peter (2003) Regulation Remixed: Institutional Change through Self- and Co-Regulation in the Mediamatics Sector, Communications and Strategies, 50(2), pp.127-157 at http://www.mediachange.ch/media//pdf/publications/Latzer_Just_Saurwein_Slominski_2004_CommStrat.pdf Latzer, Michael, Just, Natascha, Saurwein, Florian, Slominski, Peter (2006) Institutional Variety in Communications Regulation. Classification scheme and empirical evidence from Austria, Telecommunications Policy, 30(3-4), pp.152-170. Saurwein, Florian, Latzer, Michael (2010) Regulatory Choice in Communications: The Case of Content-Rating Schemes in the Audiovisual Industry, Journal of Broadcasting & Electronic Media, 54(3), pp.463-484

24 Latzer, M. (2007) Regulatory Choice in Communications Governance, European Journal of Communication, 22 (3), pp.399-405. Latzer, M. and Saurwein F. (2007) Trust in the Industry – Trust in

Co-regulation has been discussed since the late 1980s, in the Australian context as a hybrid of state and self-regulation [25]. By the mid-1990s, it had moved from a proposed technique to a detailed advertising industry rule-making procedure, with the replacement of the industry self-regulatory body by a co-regulatory scheme[26]. This was undertaken by the Australian Competition and Consumer Commission (ACCC) within its powers to exempt collective agreements under the Trades Practices Act 1974[27]. Its Code was compared with the UK self-regulatory Portman Code founded in 1989, cited as an example of independent self-regulation and praised and cited for its effectiveness by the UK government Better Regulation Executive[28]. Black states that a taxonomy of self-regulation runs from:

- mandated private regulation, within a broad framework defined by government[29];
- sanctioned private regulation, subject to government approval[30],
- coerced private regulation, «in response to threats [of]... statutory regulation», and
- pure voluntary private regulation.[31]

Huyse and Parmentier distinguish self-regulatory relationships: subcontracting in which the state sets formal conditions for rule making, but leaving it up to parties to shape the content; 'concerted action' in which the state sets both formal and substantive conditions for rule making; 'incorporation' in which existing but non-official norms become part of the legislative order by insertion into statutes[32].

---

the Users: Self-Regulation and Self-Help in the Context of Digital Media Content in the EU, Report for Working Group 3 of the Conference of Experts for European Media Policy, More Trust in Content – The Potential of Co- and Self-Regulation in Digital Media, Leipzig: 9-11 May 2007.

25 Beresford Ponsonby Peacocke, Gerald (1989) Discussion paper on industry co-regulation, New South Wales: Business and Consumer Affairs

26 Media Council of Australia (1992) A review by the Media Council of Australia of the co-regulatory system of advertising insofar as it relates to the advertising of alcoholic beverages, Media Council of Australia; Media Council of Australia (1993) Australian advertising co-regulation: procedures, structures and codes : effective October 1, 1993, Media Council of Australia

27 ACCC (2007) Authorisation no.: A91054 - A91055 Applications for authorisation in respect of a proposed Retailer Alert Scheme, 31 October, ACCC at http://www.accc.gov.au/content/trimFile.phtml?trimFileName=D07+100992.pdf&trimFileTitle=D07+100992.pdf&trimFileFromVersionId=821309

28 Prime Minister's Strategy Unit (2004) Alcohol Harm Reduction Strategy for England, March, cited at http://www.publications.parliament.uk/pa/cm200910/cmselect/cmhealth/151/15108.htm and Better Regulation Executive (2005) Routes to Better Regulation: A Guide to Alternatives to Classic Regulation Annex B: Case study 2 non-broadcast advertising, at pp.50-51, see http://archive.cabinetoffice.gov.uk/brc/upload/assets/www.brc.gov.uk/routes.pdf

29 As described in Ayres and Braithwaite (1992) Responsive regulation, in the self-enforced regulation model.

30 Ogus A. (1995) Regulation, Legal form and economic, Oxford Journal of Legal Studies, 15, p.96, describes the classic consensual regulation model.

31 Black, J. (1996) Constitutionalising Self-Regulation, Modern Law Review, Vol. 59, No. 1, pp. 24-59 at 55.

32 Huyse, L., & Parmentier, S. (1990). Decoding codes: The dialogue between consumers and suppliers through codes of conduct in the European community. Journal of Consumer Policy, 13, pp.253–272, at 260.

Within the European context, co-regulation was described by van Schooten and Verschuuren as an element of 'non state law' backed by «some government involvement» [33]. They see co-regulation as one of the emerging forms of smart regulation, alongside certification and audited standard making as an interim step between state-provided regulatory agency action and more self-regulatory forms. OECD has tried to detail the uses of co-regulation[34]. They explain that since Hart's *The Concept of Law*[35], it has been recognised that what is of interest in regulation is generally secondary rules rather than primary legislation, and that what is of interest in this secondary rule-making is how much involvement government actually devolves to private actors[36]. The variety of rules and rule-making in Internet governance describes a law that is about compliance and negotiation rather than a monopoly of force, reflecting Hart's insight. Sinclair states that no clear practical division exists between state and private self-regulation[37]. Tambini et al stated: «If part of the calculation of industry bodies involves awareness that the state might do something or be compelled to do something should they fail to take responsibility for self-regulation, then we can say that there is at least co-regulatory oversight.»[38]

The discussion of co-regulation is unsurprisingly also associated with the rise of discussions of 'governance' as distinct from 'government', which also arose in the late 1980s in political science literature, though earlier in organisational and business studies. The term 'governance' began to be used widely in political science literature in the 1990s, to describe intermediate forms of self-regulation in the post-Cold War globalization literature[39]. Varying definitions of governance have been adopted by practitioners and academics, falling into what might be termed 'minimalist' and 'maximalist' areas[40]. I use the term 'Internet

33 Van Schooten, Hanneke and Jonathan Verschuuren (2008) International governance and law: state regulation and non-state law, Cheltenham: Edward Elgar at p2.

34 OECD (2006) Interim Report on Alternatives to traditional regulation: Self-regulation and Co-Regulation, Working Party on regulatory management and reform, Paris, OECD.

35 Hart, H.L.A. (1961) The Concept of Law, Clarendon Press, Oxford

36 See van Schooten supra n.34 at p.65.

37 See Sinclair D. (1997) Self-regulation Versus Command and Control? Beyond False Dichotomies. Law & Policy 19(4), pp.529-559.

38 Tambini, Damian, Danilo, Leonardi, and Marsden, Chris (2007) Codifying Cyberspace: Self Regulation of Converging Media Cavendish Books. London: Routledge, at p43.

39 Pierre, J. (2000) Introduction: Understanding Governance in Pierre, J. (ed.) Debating Governance: Authority, Steering and Democracy, Oxford University Press. The term was earlier used in Jones, C. & Hesterly, W.S. (1993) Network organization: An alternative governance form or a glorified market? Academy of Management Meetings, Atlanta, Georgia.

40 For a maximalist position that places all existing regulation plus informal modes of governance into the over-arching description, see the broad use in Zysman, J. and Weber, S. (2000) Governance and Politics of the Internet Economy—Historical Transformation or Ordinary Politics with a New Vocabulary? BRIE Working Paper 141, E-conomy Project Working Paper 16 also in N.J. Smelser and P.B. Baltes, eds. (2000) International Encyclopedia of the Social & Behavioral Sciences, Elsevier Science Limited, Oxford.

regulation' to refer to the range of public-private interactions covering substantive national and regional-plurilateral rules and practices governing specific Internet topics[41]. Regulation as a rules-based field existing within a wider policy discussion of governance is the approach outlined for legal scholars[42]. Governance is further discussed in much of the political science literature in terms of networks and informal rule-making institutions such as multinational corporations and - particularly relevant for Internet governance - standard-setting organisations[43]. Governance as a concept explains the networked modes of regulating[44], by the governments concerned, by market actors in collaboration, by civil society stakeholders. The position adopted by the United Nations[45] distinguishes direct Internet governance mechanisms from those that more properly are placed within telecommunications or media law. The EC 2001 *Governance* White Paper intended to: «adopt new forms of governance that bring the Union closer to European citizens, make it more effective, reinforce democracy in Europe and consolidate the legitimacy of the institutions.» [46] The politics of governance research accompany the legal study of co-regulation.

The European co-regulation approach was detailed in 2002[47]. It became official policy in 2003 and defined co-regulation as: «the mechanism whereby a Community legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognised in the field (such as economic operators, the social partners, non-governmental organisations, or associations)…[parties] may conclude voluntary agreements for the purpose of determining practical arrangements... the Commission will verify whether or not those draft agreements comply with Community law (and, in particular, with the basic legislative act).» [48] Paragraph 21 sets out in some detail the types of monitoring needed: «The competent legislative authority will define in the act the relevant measures to

41 Marsden, C ed. (2000), and for the broader policy approach Grewlich, K. (1999) Governance in 'cyberspace': access and public interest in communications, Amsterdam: Kluwer.

42 Scott, Colin (2004), Regulation in the Age of Governance: The Rise of the Post-regulatory State, in Jordana, Jacint and David Levi-Faur (2004) The Politics of Regulation, Cheltenham: Edward Elgar.

43 See recently Christou and Simpson (2009) New Modes Of Regulatory Governance For The Internet? Country Code Top Level Domains In Europe, http://regulation.upf.edu/ecpr-07-papers/ssimpson.pdf

44 For forms of regulation far removed from government, see Benkler, Y. (2006) The Wealth of Networks, Yale University Press

45 See United Nations (2005) Working Group on Internet Governance Final Report.

46 EC (2001) White Paper on European Governance at http://ec.europa.eu/governance/white_paper/en.pdf

47 COM(2002)275 European Governance: Better Lawmaking, 5 June, COM/2002/0278 Action plan Simplifying and improving the regulatory environment, COM 2002/704 Towards a reinforced culture of consultation and dialogue - General Principles and minimum standards for consultation of interested parties by the Commission, 11 December

48 Inter-Institutional Agreement on Better Law-Making, Official Journal of the European Union December 2003, 2003/C 321/01 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2003:321:0001:0005:EN:PDF, at Paragraphs 18-20.

be taken in order to follow up its application.» This suggests substantial work programmes on compliance and adaptation of the legislative act in the case of co-regulation, where the Commission monitors co-regulation[49].

The Commission also sets out the circumstances in which forms of regulation short of state regulation will not be constitutionally appropriate «where fundamental rights or important political options are at stake or in situations where the rules must be applied in a uniform fashion in all Member States.» Howells asked: «who will decide what is so unimportant that it can be decided by co-regulation?»[50] This is particularly the case where human rights law is increasingly being applied by commercial actors (such as ISPs) in various forms. It is self-evident that the more supervision and review resembles that in full state regulation, the less the benefits of flexibility and industry participation. Self- and co-regulation must also not infringe principles of competition or «the unity of the internal market».

Academic authors have been somewhat cynical about the constitutional legitimacy and representation in co-regulation[51], especially as regards industry Codes of Conduct that are supported by government agencies, but Collins maintains that the 'Social Dialogue' has helped create «labour law [as] the field in which co-regulation has been most successful» [52], explaining «self-regulation [success] has only been [under] the credible threat of imminent action by the [European] Council.»[53] Moreover, the Court of First Instance has established that co-regulation is only legitimate where the «representativeness» of relevant stakeholders is well displayed[54]. The European Commission in 2005 analyzed co-regulation in terms of 'better regulation'[55]. This was immediately made part of internal EC practice[56] which the Commission must follow before bringing forward a new legislative or policy proposal. However, supervision and judicial review is still a necessary fudge in co-regulatory decision-making. The devil lies in the detail of co-regulation and its observance of constitutional law, which I now explore in the Internet context.

---

49 For example, COM(2009) 504 Report From The Commission On Subsidiarity And Proportionality (16th report on Better Lawmaking covering the year 2008) at http://ec.europa.eu/governance/better_regulation/documents/com_2009_0504_en.pdf

50 Howells, G. (2004) Co-regulation's Role in the Development of European Fair Trading Laws, Chapter 5 pp.119-130 in Bussani, M. And Mattei, U. The Common Core in European Private Law, Amsterdam: Kluwer.

51 Scott, J. And Trubek, D.M. (2002) Mind the Gap: Law and New Approaches to Governance in the European Union, 8 ELJ 1.

52 Collins, Hugh (2004) EC Regulation of Unfair Trading Practices, Chapter 1 pp.1-41 in Bussani, M. And Mattei, U. The Common Core in European Private Law, Amsterdam: Kluwer.

53 Ibid at p33. See further Joerges, C., Y. Meny, and J.H.H. Weiler (2001) Responses to the European Commission's White Paper on Governance, European University Institute: Florence.

54 UEAPME v. Council (1998) Case T135/96, ECR II-2335.

55 COM (2005) 97 Better Regulation for Growth and Jobs in the EU

56 SEC (2005) 791 Impact Assessment Guidelines

3. TOWARDS A NUANCED TYPOLOGY OF CO-REGULATION

Case studies suggest that co-regulatory success is mixed and many factors can jeopardise its success. Verhulst and Latzer provide excellent analysis of the types of co-regulation beginning to develop and their institutional path dependency[57]. Self-regulatory bodies form as single issue bodies, often crisis-driven. There are different incentives for self-regulation, and economic as well as political analysis is needed, together with attention to the loss of constitutional guarantees[58]. Latzer identifies five types of regulation short of statutory agency-led regulation, the latter pair being prevalent in Internet content regulation:

1. Co-regulation,
2. State-supported self-regulation,
3. Collective industry self-regulation,
4. Single company self-organisation,
5. Self-help/restriction by users including rankings to impose restrictions on access to content.

He notes the direction of travel: both bottom-up transformations from self- into co-regulatory bodies, and top-down delegation from regulation into co- (but not self-) regulation. He also notes examples of what I describe as 'Potemkin' self-regulators[59], where there was a website and the appearance of a regulator but few resources, no physical address containing offices and little or no apparent adjudication and enforcement. Price and Verhulst focussed on AOL and internal self-organisation[60]. They identified increasing realism in recognising competition problems, emerging monopolies and dominance. Baird suggested that the 'bottom-up' approach from national regulation does not negate the vital role of government

57 Latzer, Michael, Price, Monroe E., Saurwein, Florian, Verhulst, Stefaan G. (2007) Comparative Analysis of International Co- and Self-Regulation in Communications Markets, Research report commissioned by Ofcom, September, Vienna: ITA at www.mediachange.ch/media//pdf/publications/latzer_et_al_2007_comparative_analysis.pdf

58 See formal regulatory elaborations at: Ofcom (2004) Criteria for promoting effective co and self-regulation: Statement on the criteria to be applied by Ofcom for promoting effective co and self-regulation and establishing coregulatory bodies www.ofcom.org.uk/consult/condocs/coreg/promoting_effective_coregulation/co_self_reg.pdf
Ofcom (2006) Online protection: A survey of consumer, industry and regulatory mechanisms and systems, www.ofcom.org.uk/research/technology/onlineprotection/report.pdf
Office of Regulation Review (1998) A Guide to Regulation, Second Edition, December 1998 at www.pc.gov.au/orr/reguide2/reguide2.pdf
Oftel (2001) The Benefits of Self and Co-regulation to Consumers and Industry, at www.oftel.gov.uk/publications/about_oftel/2001/self0701.htm

59 In the original 'Potemkin' villages, General Potemkin (or Potyomkin) infamously created facades of villages in 1787 to present an image of prosperity to Empress Catherine II of Russia, in which there was no substance to the buildings, a myth for which a website of equally contested veracity provides discussion http://en.wikipedia.org/wiki/Potemkin_village

60 Price and Verhulst (2005) Self Regulation And The Internet.

– in fact she suggests that they are clearly the leading policy player[61]. Millwood-Hargrave also defines the progress from self- to co- to state regulation.[62]

The UK Better Regulation Executive has itself described co-regulation in detail, and has broken down eight elements short of 'classic' regulation that can enable regulatory compliance, including 'New Approach' Directives (which permit compliance via standards) and flexible Directives (its example being the revised Audio Visual Media Services Directive) which permit wide discretion in the manner and form of implementation[63]. They claim the advantage of co-regulation «is that it provides a degree of certainty due to the backstop legal provisions whilst also encouraging innovation by allowing a flexible approach to implementation» and claim that «Co-regulatory initiatives are more likely to be successful as those being regulated have scope to use their experience to design and implement their own solutions.»[64] Ofcom's regulatory analysis of co- and self-regulation conducted in 2008 arrives at similar conclusions[65].

Following a multi-year empirical investigation with a multinational research team, I analyzed the previous literature on Internet co- and self-regulation, identified case studies, and established twelve states of regulation from the 'purity' of standard setting self-regulation to a form so close to regulation that the regulator itself internally recognises the form as effectively regulation. Combining Latzer's approach with Verhulst's leads to Table 1.

Table 1: Twelve Ideal Types of Self- and Co-regulation[66]

Regulatory Scheme	Illustrative Example	Scale	Government Involvement
'Pure' unenforced self-organisation	SecondLife	0	Informal interchange only – evolving partial industry forum building on players' own terms
Acknowledged self	Bebo Creative Commons	1	Discussion but no formal recognition/approval
Ex post standardised self	W3C#	2	Ex post approval of standards

61 Baird Zoe (2002) Governing the Internet: Engaging Government, Business, and Nonprofits, Foreign Affairs, November/December 2002, p.81 at www.foreignaffairs.com/articles/58427/zoe-baird/governing-the-internet-engaging-government-business-and-nonprofi.

62 Millwood-Hargrave, M. (2007) Report for Working Group 3 of the Conference of Experts for European Media Policy, More Trust in Content – The Potential of Co- and Self-Regulation in Digital Media, Leipzig: 9-11 May.

63 BRE (2005) at 6.

64 BRE (2005) at 26.

65 See Ofcom (2008) Identifying appropriate regulatory solutions: principles for analysing self and co-regulation, Ofcom, 10 December 2008, largely the work of Tom Kiedrowski.

66 Adapted from: Cave, J., Marsden C. and Simmons, S. (2008) Phase 3 (Final) Report Options for and Effectiveness of Internet Self- and Co-Regulation, TR-566, RAND Corp: Santa Monica, CA. at p.xii.

Regulatory Scheme	Illustrative Example	Scale	Government Involvement
Standardised self	IETF	3	Formal approval of standards
Discussed self	IMCB	4	Ex ante informal consultation – but no sanction/approval/process audit
Recognised self	ISP Associations	5	Recognition of body – informal policy role
Co-founded self	FOSI#	6	Ex ante negotiation of body; no outcome role
Sanctioned self	PEGI#	7	Recognition of body – formal policy role (contact committee/process)
Approved self	IWF#	8	Ex ante informal negotiation with government –with recognition/approval
Approved compulsory co-regulatory	ICANN	9	Ex ante negotiation with government –with sanction/approval/process audit
Scrutinised co-regulatory	NICAM# ATVOD	10	As 9 with annual budget/process approval
Independent Body (stakeholder forum)	PhonePayPlus NOMINET	11	Government imposed and co-regulated with taxation/compulsory levy

Note that these approximate classifications do not relate to degree of government funding – the relationship between direct or indirect government funding is not consistent with policy involvement. For instance, government may choose to support a self-regulatory standard-setting activity as a genuinely deregulatory policy, as in Scales 2 and 6. That may include government financial support or co-funding. One can investigate whether such approaches are consistent with policy support via the success or failure of proposed policy interventions to extend the scope of such bodies.

4. CONSTITUTIONAL REVIEW AND CO-REGULATION

Having identified types of co-regulation, with varying degrees of government formal involvement and therefore potential public scrutiny, we can investigate the extent to which constitutional courts have intervened in such co-regulatory game-playing, and found a need for greater legitimacy in the rules proposed. Cafaggi states in regard to sanctioned regulation: «An intermediate hypothesis between delegated private regulation and ex post recognized private regulation is that in which private regulation, produced by the private or self-regulator, has to be approved by a public authority to become effective.»[67] The decision on recognition is binary. Cafaggi points out that the recognition is of the standard, not of the

67 See Cafaggi, F. (2006) Rethinking private regulation in the European regulatory space, EUI Working Paper LAW No. 2006/13, at http://cadmus.eui.eu/bitstream/handle/1814/4369/LAW2006.13.PDF?sequence=1 at p.24.

process or the regulator, which leaves much greater discretion for both sides. Moreover, he indicates that *Wouters* may prove the basis for the ECJ to decide more minutely the application of competition law to self-regulation[68].

MacSithigh states that «self-regulation retains its allure in some sectors (particularly media and communications), as it neatly side-steps complaints of State interference and keeps the costs of regulation off the public books»[69] even if that incurs costs for private actors dealing with such quasi-public bodies as the Press Complaints Commission (PCC) and Internet Watch Foundation (IWF). This is unsatisfactory in the 'Regulatory State'[70] with the devolution of authority from public to private bodies, in which the Internet is a particular exhibit of interest: almost every function in Internet content regulation is 'contracted out' or otherwise left to self-regulation. For instance, IWF considers itself bound by its constitution as a charity, not by its potential public authority status. Note that private bodies with public functions have proved controversial in tortuous liability terms[71].

European examples of co-regulation now abound in this field, notably in Internet security but also in child safety and filtering, as well as standard setting and social network privacy regulation[72]. President Sarkozy of France has made it clear that government needs to further tighten its grip on the Internet[73]. Both soft law and soft enforcement play a vital regulatory role which legal positivists would be in danger of overlooking or minimizing by a failure to consider the

68 Case C-309/99 J.C.J.Wouters et al v. Algemaane Raad van de Nederlandse Orde van Advocaten [2002] ECR I-1577, stating that «According to its very wording, Article 85 of the Treaty applies to agreements between undertakings and decisions by associations and undertakings. The legal framework within which such agreements are concluded and such decisions taken, and the classifications given to that framework by their various national legal systems are irrelevant as far as the applicability of the Community rules on competition and in particular Article 85 of the Treaty are concerned» (para 66). See the argument that Wouters is only a useful precedent for judicial non-activism in licensing rules for the 'liberal professions' rather than wider self-regulation, in Forrester, Ian (2004) Where Law Meets Competition: Is Wouters Like a Cassis de Dijon or a Platypus? EUI Competition Conference 2004, at http://www.eui.eu/RSCAS/Research/Competition/2004/200409-compet-Forrester.pdf

69 MacSithigh, Daithi (2009) Datafin to Virgin Killer: Self-Regulation and Public Law, Norwich Law School Working Paper No. NLSWP 09/02 at p.3 at http://ssrn.com/abstract=1374846 See also MacSithigh, Daithi (2008) The Mass Age of Internet Law, Information and Communication Technology Law, Vol. 17, No. 2, pp. 79-94 at http://ssrn.com/abstract=1271863

70 Majone, G. (1999) The Regulatory State and its Legitimacy Problems, West European Politics, 22(1), pp.1-24.

71 See Cornford, T. (2008) Towards a Public Law of Tort, Ashgate Publishing, especially Chapter 2, pp.9-16.

72 See the pertinent case studies and their challenge to offline media law in MacSithigh, D. (2008) The Mass Age of Internet Law, Information and Communication Technology Law, Vol. 17, No. 2, pp. 79-94.

73 Sarkozy, N. (2010) Speech to the Embassy of France to the Holy See, reported in Moya, J. (2010) French Pres: Increased Net Regulation is «Moral Imperative», Zeropaid, 11 October, at http://www.zeropaid.com/news/90997/french-pres-increased-inet-regulation-is-moral-imperative/?utm_source=twitterfeed&utm_medium=twitter

law in its regulatory context. Newman and Bach state: «In the U.S., the government induces self-regulation largely through the threat of stringent formal rules and costly litigation should industry fail to deliver socially desired outcomes…We label the ideal-typical U.S. model legalistic self-regulation.»[74] This 'private interest government' is a model readily observable in Internet regulation, and accepted with conditions by the US courts in for instance *National Association of Broadcasters*[75]. Recently, influential scholar and sometime administration official Weiser has proposed Internet co-regulation, to construct network neutrality principles, the control over ISP throttling and blocking of content, while acknowledging that this is a radical and foreign practice for US regulators[76]. Recognising its useful compromise between legitimacy and flexibility in view of the Ofcom 2008 study, he proposes an adaptation of the European approach which I outlined in a previous monograph[77]. Froomkin's earlier detailed examination of the domain name system and private governance, explains how the form of co-regulation for ICANN adopted by the United States government prevented the constitutional legitimacy and scrutiny afforded to all other regulatory agencies by the Administrative Procedure Act[78].

The nature of a public body in the UK, was extended by the Human Rights Act 1998 ('HRA'), whose relevant (non)definition in s.3 is: «(a) a court or tribunal, and (b) any person certain of whose functions are functions of a public nature.» In s.5 it further delimits the definition: «a person is not a public authority by virtue only of subsection (3)(b) if the nature of the act is private.» Various cases have established that the mere nature of a contract with government authority does not qualify the private body as public, so mere Heads of Agreement or mutual recognition of a private self-regulatory body with a government agency will not necessarily give grounds for claiming its 'public' nature. While there are moves to designate public bodies more widely under European and UK law, no significant change that would affect the status of such charitable self-regulatory bodies appears likely.

The government broadly expects equivalence between definitions of public bodies under HRA[79], case law on judicial review under the Supreme Court Act 1981, and Freedom of

74 Newman Abraham L. and David Bach (2004) Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States, Governance: An International Journal of Policy, Administration, and Institutions, Vol. 17, No. 3, July 2004 pp. 387–413 at p.388.

75 National Association of Broadcasters v. F.C.C. (1976) 180 U.S.App.D.C. 259, 265, 554 F.2d 1118, 1124. See also Writers Guild Of America, West, Inc. v. F.C.C., (1976) 423 F. Supp. 1064.

76 Weiser, P. (2009) The Future of Internet Regulation, 43 U.C. Davis L. Rev. pp.529-590 at p.583 comparing securities with telecom s regulation, also at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1344757

77 Marsden, C. (2010) Net Neutrality: Towards a Co-regulatory Solution, Bloomsbury Academic: London, repeating and elaborating on conclusions from earlier work.

78 Froomkin, A. Michael (2000) Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution, 50 DUKE L.J. 17 2000, also at http://www.law.miami.edu/~froomkin/articles/icann.pdf.

79 On the growth of modern human rights law more generally, and Essex Human Rights Centre's contribution to it, see Boyle, K. (2008) Twenty-Five Years of Human Rights at Essex, Essex Human Rights Review Vol. 5 No. 1 July, pp1-15.

Information Act 2000[80]. MacSithigh notes that the Information Commissioner was pressed to include the Press Complaints Commission and premium telephone regulator PhonePay-Plus within 'public authorities', and the BBC already has been so designated by the Supreme Court[81]. Ofcom's use of non-legal instruments, notably the Broadcasting Code for its licensees, has been found reviewable in *R. (Gaunt) v. Ofcom*[82]. John Gaunt was summarily dismissed from his TalkSport radio presenting contract for breaching the Ofcom broadcast code. Ofcom found breaches of Regulations 2.1 and 2.3 of the Code under the Communications Act 2003. Gaunt claimed that Ofcom's finding was a disproportionate interference with his freedom of expression and an infringement of his human rights. The court found for Ofcom, though finding that proportionality of the Code and its enforcement was reviewable.

Horizontal indirect effect is predicted to become more extensive than direct effect, as s.6(1) and s.6(3)(a) HRA provides a limit to review of public bodies, while at least in theory common law is enabled to take an unlimited liability towards human rights for private bodies as well as public[83]. Note the deference paid to public bodies in judicial review still continues, if somewhat weakened since HRA[84]. S.6(3)(b) also applies to 'any person certain of whose functions are functions of a public nature' within the definition of a public authority, making it unlawful for that body to contravene Convention rights when performing a public function[85]. European Community law, by contrast, limits the effects on individuals[86].

---

80 Justice, Ministry of (2007) Consultation Paper CP 27/07 at Paragraph 19, see www.justice.gov.uk/docs/cp2707.pdf

81 BBC v. Sugar [2009] UKHL 9, noting that Part IV of schedule 1 to the Freedom of Information Act 1998 provides that the BBC is a 'public authority' 'in respect of information held for purposes other than those of journalism art or literature', which in this case meant disclosure under s.50(3) of the Act was required to be always considered. The Commissioner thus must treat hybrid authorities as always being 'public authorities' for the purposes of Section 1, irrespective of the nature of the requested information.

82 R. (Gaunt) v Ofcom (Liberty intervening) [2010] EWHC 1756 (Admin); [2010] WLR (D) 180 at http://www.lawreports.co.uk/WLRD/2010/QBD/R(Gaunt)_v_Ofcom.html

83 Phillipson, G. (1999) The Human Rights Act, «Horizontal Effect» and the Common Law: a Bang or a Whimper? 62 Modern Law Review 824; T Raphael (2000) The Problem of Horizontal Effect, European Human Rights Law Review p.493; Phillipson, G. (2007) Clarity Postponed: Horizontal Effect after Campbell, p.143 in Fenwick, Masterman and Phillipson (eds) Judicial Reasoning under the UK Human Rights Act, Cambridge University Press.

84 For media and communications regulation to 1996, see Marsden, C. (1999) Judicial Review and Regulation of UK Analogue and Digital Commercial Terrestrial TV Licensing: Shotgun Marriage and Divorce in a Very British Affair 10 Utilities Law Review 3, pp.125-144.

85 Poplar Housing and Regeneration Community Association Limited v Donoghue (Poplar Housing) [2001] EWCA Civ 595 – wherein a housing association providing the local authority's duty to provide homeless with shelter was found to be performing the local authority's function and thus subject to review.

86 Young, Alison L (2009) Human Rights, Horizontality and the Public/Private Divide: Towards a Holistic Approach, University College London Human Rights Law Review 1: 159-187 states (p.162) that «This contrasts with the position in European Community law, where the obligation to interpret na-

The distinction drawn in *YL*[87] by the Supreme Court majority is critical, in narrowly defining public function to 'mirror'[88] the European Court of Human Rights (ECtHR) jurisprudence: «A private body would be regarded as performing a public function were it to exercise a governmental function, wielding coercive powers»[89].

Breaches of the tort of privacy have been held to be subject to obligations on private actors in several cases, *Campbell*, *Murray* and *McKennitt*[90]. This only affects regulatory organisations inasmuch as they publish details of complaints and cases adjudicated, but *Campbell* in particular is a construction, not a 'mirror' to the ECtHR's jurisprudence[91], unless one accepts the controversial decision in *Von Hannover*[92] as good authority. Not only have English courts prescribed reporting by private media organisations above and beyond the ECtHR, they have also restricted its alter ego, the right to freedom of expression under Article 10 ECHR in the case of public bodies, in *Pro Life v. BBC* and *Animal Defenders International*[93]. This restrictive attitude to free speech – deferring to Parliamentary will - has been noted by several scholars, as Parliament expressly delegated to BBC judgment in matters of taste and decency, and noted in a S.19(1)(b) statement that its restrictions on political advertising could be contrary to the ECHR[94].

---

tional law in a manner compatible with European Community law does reach a limit when this requires the creation of an obligation in criminal law, or a heightening of a criminal penalty», citing C-80/86 Kolpinghuis Nijmegen [1987] ECR 3969 and C-387/02 Silvio Berlusconi [2005] ECR I-3565.

87 YL (Appellant) v. Birmingham City Council and others [2007] UKHL 27 on appeal from: [2007] EWCA Civ 27, see http://www.publications.parliament.uk/pa/ld200607/ldjudgmt/jd070620/birm-1.htm

88 For the 'mirror principle', see Lewis, J. (2007) The European ceiling on Human Rights, Public Law p.720 and Lewis, J. (2009) In re P and others: an exception to the 'no more and certainly no less' rule, Public Law p.43

89 YL (2007) per Lords Scott, Mance and Neuberger. This narrow interpretation was followed in London and Quadrant Housing Trust v R. (on the application of Weaver)(Weaver) [2009] EWCA Civ 587; [2009] All ER (D) 179 (Jun), further restricting rights by focusing on the definition of private acts in s.6(5) of the HRA 1998, the nature of the act and the function performed.

90 Campbell v Mirror Group Newspapers plc [2004] UKHL 22, [2004] 2 AC 457 [15]; McKennitt v Ash 37 [2006] EWCA Civ 1714; [2007] 3 WLR 194; Murray v Express Newspapers Plc [2008] EWCA Civ 446, [27];[2008] 3 WLR 1360;.

91 See Moreham, N. (2006) Privacy in Public Places, 65 Cambridge Law Journal p.606; Rudolf, B. (2006) Case Comment: Von Hannover v Germany, 4 International Journal of Constitutional Law p.533; Hatziz N. (2005) Giving Privacy its due: private activities of public figures in Von Hannover v Germany, 16 King's College Law Journal p.143.

92 Von Hannover v. Germany ECHR 59320/00; (2004) 16 EHRC 545

93 R. (ProLife Alliance) v British Broadcasting Corporation (ProLife) [2003] UKHL 23; [2004] 1 AC 185; R. (Animal Defenders International) v Secretary of State for Culture, Media and Sport (ADI) [2008] UKHL 15; [2008] 1 AC 1312

94 Barendt, E. (2003) Free Speech and Abortion, Public Law p.580; Lewis T. and P Cumper, P. (2009) Balancing freedom of political expression against equality of political opportunity: the courts and the UK's broadcasting ban on political advertising, Public Law 89

5. CONSTITUTIONAL PROTECTION BY THE EUROPEAN CHARTER OF FUNDAMENTAL RIGHTS

Greater scrutiny will prove important in future judicial assessment of co-regulatory forms, an area that is rapidly becoming a focus for both national courts[95] and the European judicial process, both the European Court of Human Rights[96] and CJEU[97]. The European Charter of Fundamental Rights, incorporated in 2010, serves up a web of conflicting rights for citizens and responsibilities on governments, now made European law by the Treaty of Lisbon from 1 December 2009[98]. The CJEU found in 2010 that the Charter of Fundamental Rights, which incorporates the European Convention on Human Rights into European Union law, could be used to strike down secondary legislation which fails to respect the rights of individuals to privacy[99]. The CJEU refused to consider a broader question about the implementation of the Data Retention Directive[100], which would have set a much broader precedent for national courts to consider European law against Charter rights. This

95 Though note UK courts continue a non-interventionist approach, as seen in the judicial review of the Digital Economy Act [R. (British Telecom & TalkTalk) v Secretary of State for Business, Innovation and Skills [2011] EWHC 1021 (Admin)], and the recent judgment extending copyright enforcement against a third-party intermediary ISP: Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc [2011] EWHC 1981 (Ch).

96 See Council of Europe (2008) Human rights guidelines for Internet service providers, H/Inf 2008 (9) Council of Europe, Strasbourg in co-operation with the European Internet Services Providers Association at http://www.coe.int/t/informationsociety/documents/HRguidelines_ISP_en.pdf, , a short summary of rights as a guide for Internet Service Providers, with extracts from previous Council of Europe recommendations attached as an annex, a useful guide to Council of Europe work in the Internet area, with regard to both privacy and freedom of expression under the European Convention. See further Brown, I. and Korff, D. (2011) Social Media, Political Activism and Human Rights, Issue Paper for the Council of Europe Commissioner for Human Rights at http://ssrn.com/abstract=1860060, a survey of relevant instruments and case law under the European Convention, together with leading academic surveys conducted to support analysis of human rights as applied to social media and political speech on the Internet, arguing for reducing the 'margin of appreciation' in member states' censorship of the Internet to encourage wider protection of political speech.

97 See C-42/07 Liga Portuguesa de Futebol Profissional v. Departmento de Jogos [2009] ECR 1 [2010] 1 CMLR 1 ECJ.

98 Charter Of Fundamental Rights Of The European Union (2010/C 83/02) at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF

99 C-92/09 and C-93/09 (2010) 9 November Joined Cases Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) v. Land Hessen. For commentary see Content and Carrier (2010) «break no privilege nor charter»: ECJ invalidates regulations for breaching Charter of Fundamental Rights, at http://www.contentandcarrier.eu/?p=413

100 C-92/09 Paragraph 38: «the referring court asks the Court to rule on the validity of Directive 2006/24 and on the interpretation of Article 7(e) of Directive 95/46, so as to enable it to assess whether the retention of certain data relating to the users of the internet sites, laid down by European Union and German legislation, is lawful.»

may come back to the CJEU in a Swedish Supreme Court referral (*Perfect Communication AB*[101]) to be heard in 2012.

The E-Commerce Directive (ECD) of 2000 enshrined the principle of the Internet host 'safe harbour' of non-liability, and leaves much detailed co-regulation to the market actors (mainly ISPs) in Codes of Conduct[102]. Benoit and Frydman establish that it was based on the 1997 German Teleservices Act[103], and contrast it with forms of co-regulation in the United States and China[104]. Frydman and Rorive observe that US courts had always «in line with the legislative intent…applied the immunity provision in an extensive manner»[105]. In Europe, a patchwork of different national co-regulatory arrangements based on the national legal implementation of the ECD is increasingly subject to CJEU. CJEU in its 2011 *l'Oréal v. eBay* judgment[106] began to circumscribe the degree of co-regulatory censorship exercised by ISPs in response to content owners' requests for allegedly infringing material to be removed, the first in a much more extensive series of cases before the CJEU. (It is instructive to note that since the US Supreme Court ruled in *ACLU v. Reno* in 1997[107], it took over a decade for the CJEU to fully consider ISP liability for third party violation of intellectual property rights (IPRs) against constitutional rights to free expression and privacy of personal data, in *Scarlet Extended*[108]).

In *Scarlet Extended*, the CJEU had to balance copyright holders against ISP and users' rights. The CJEU recognised that risk of preventing access to lawful content through over-blocking or overfiltering is a relevant factor to take into account. Paragraphs 43-44 in *Scarlet Extended* are general guidance:

---

101 Case C-461/10: Reference for a preliminary ruling from the Högsta domstolen (Sweden) lodged on 20 September 2010 — Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget Aktiebolag, Storyside AB v Perfect Communication Sweden AB, OJ C 317 , 20/11/2010 P. 0024 – 0024 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62010P0461C(01):EN:HTML

102 See Article 1(1)(2), Article 16 and Recitals 32, 49, of 2000/31/EC.

103 German Teleservices Act 1997 (TDG («Federal Act Establishing the General Conditions for Information and Communication Services» of July 22, 1997, BGBl. I S. 1870)

104 Frydman, B, Hennebel, L and Lewkowicz, G. (2008) Public Strategies for Internet Co-Regulation in the United States, Europe and China. SSRN http://ssrn.com/abstract=1282826 posted 20 June 2009; also Chapter 6 'Co-regulation and the rule of law' in Eric Brousseau, Meryem Marzouki, Cécile Méadel (2012) Governance, Regulations And Powers On The Internet. Cambridge: Cambridge University Press

105 Frydman, B. and Rorive, I. (2002) Regulating Internet Content Through Intermediaries in Europe and the USA, Zeitschrift fur Rechtssoziologie Bd.23/H1, July 2002, Lucius et Lucius.

106 Case C-324/09 L'Oreal SA & Others v eBay International AG & Others, decided 12 July 2011.

107 American Civil Liberties Union v. Reno (1997) 21 U.S. 844 of June 27 No. 96-511.

108 Case C-70/10 Scarlet Extended SA v Société Belge des auteurs, compositeurs et éditeurs (SABAM) OJ C 113, 1.5.2010: 20–20. Decided 24 November 2011, OJ C 25/6, 28.1.2012. http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=EN&mode=doc&dir=&occ=first&part=1&cid=574684

> «The protection of the right to intellectual property is indeed enshrined in Article 17(2) of the Charter of Fundamental Rights of the European Union ('the Charter'). There is, however, nothing whatsoever in the wording of that provision or in the Court's case-law to suggest that that right is inviolable and must for that reason be absolutely protected.
>
> «[44] As paragraphs 62 to 68 of the judgment in *Promusicae*[109] make clear (sic), the protection of the fundamental right to property, which includes the rights linked to intellectual property, must be balanced against the protection of other fundamental rights.»

CJEU stated that the Belgian injunction in issue would be a serious infringement of the freedom of the ISP concerned to conduct its business, since it would require that ISP to install a complicated, costly, permanent computer system at its own expense. The Belgian court's order would have emasculated Art.15 ECD[110]. This reasoning was reconfirmed and extended to social networking sites by the February 2012 decision in *SABAM v. Netlog*[111].

Scarlet Extended is a short decision (as is *Netlog*): the question asked was set at the most extreme end of the scale, an injunction that was (a) preventative (b) entirely at the ISP's expense; (c) for an unlimited period; (d) applied to all customers indiscriminately; (e) for all kinds of communications. Useful statements in the judgment included that the complexity/cost of the proposed Belgian system weighed against it, that IP addresses are personal data, that the Belgian injunction was overbroad and could interfere with lawful as well as unlawful use[112].

I now briefly analyze recent national court decisions in regard to the non-judicial removal of alleged persistent online infringers of copyright. In the United Kingdom, 'graduated response' was seen as an attractive option by both outgoing Labour and incoming Conservative administrations, and the Digital Economy Act (DEA) ss.9-18 offers two new possibilities:

- acting against individuals, if copyright infringement may be detected via a router they control;
- a potential new power which can be granted by consent of Parliament under s.17 to «by regulations make provision about the granting by a court of a blocking injunction

109 Case C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU, Judgment of 29 January 2008 [2008] ECR I271

110 See European Commission (2010) Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC), at http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/questionnaire_%20e-commerce_en.pdf

111 Case C-360/10 *SABAM v. Netlog*, decided 16 February 2012, reported at http://curia.europa.eu/juris/document/document.jsf?text&docid=119512&pageIndex=0&doclang=EN&mode=req&dir&occ=first&part=1&cid=158253

112 See Scarlet supra n.10 at Paragraph 52: «injunction could potentially undermine freedom of information since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications» See further *SABAM v. Netlog* supra n.74 at paragraphs 36-38.

in respect of a location on the internet which the court is satisfied has been, is being or is likely to be used for or in connection with an activity that infringes copyright.»[113]

This potential S.17 power (as well as the overall graduated response scheme) was challenged by ISPs BT and TalkTalk. They argued that under the ECD, the role of ISPs was «passive» as mere conduits. They also argued that IP addresses of their users are personal data. The High Court at first instance dismissed most of the ISP claims, but chose to move the cost burden of the co-regulatory scheme in favour of ISPs[114]. Arguably, this helps make it '*Scarlet Extended* proof' as it ensures costs are more reasonably allocated on the rightsholders. BT/TalkTalk successfully appealed the first instance judgment in October 2012 on all grounds except Article 15 ECD[115]. The appeal was expected to be further appealed to the Supreme Court later in 2012, and possibly onward to the CJEU in 2013.

French Law n° 2004-575 relating to trust in the digital economy, Article 6 paragraph I–1 states that: «Persons whose activity consists in providing public access to online communication services must inform their subscribers of the existence of technical means to limit access to certain services or must select and provide their subscribers with at least one of these means» [116]. In addition to this mandating of ISPs to educate users about blocking services, in 2009 the French anti-piracy law introduces 'graduated response' against illegal content downloading:

1. HADOPI, the body created for this purpose, will send the infringer a warning e-mail.
2. If the infringement is repeated within 6 months, a new e-mail is sent together with a warning by registered letter.
3. If the infringement is repeated within a year, the Internet user is penalised according to the gravity of the act.

The sanction can be the denial of Internet access ranging from one month to a year during which time the Internet user must continue to pay the ISP subscription and is included on a black list that forbids her to subscribe to any other ISP. The passage of

113 Note the powers for rightsholders compared with S.97(A) CDPA: 97A requires that the service provider's service «is being used» to infringe copyright (present tense); S.17 works even if infringement stopped forever and also if there has not yet been any infringement but it is likely to happen. S.97A requires service provider to know about infringement, section 17 does not. Under S.17 a web location blocked may not be guilty of copyright infringement, but may merely be used to facilitate access to locations that are. S.97A may not be used to prevent access to sites that are not themselves infringing. S.17 DEA is thus much wider than S.97A – if implemented!

114 British Telecommunications Plc R (on the application of) v Secretary of State for Business, Innovation and Skills [2011] EWHC 1021 (Admin).

115 BT Plc & Another, R (on the application of) v Secretary of State for Business, Innovation and Skills [2011] EWCA Civ 1229 (7 Oct).

116 For background and analysis see Meyer, Trisha & Leo Van Audenhove (2011) Surveillance and regulating code: An analysis of graduated response in France, Cyber-Surveillance In Everyday Life: An International Workshop * May 12-15, 2011 * University of Toronto at http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Meyer-Audenhove-Regulating-code.pdf

the 'HADOPI law'[117] on 13 May 2009 was immediately referred by sixty members of the French parliament to the Constitutional Court, which on 10 June struck down the elements of the law which create a punishment prior to judicial instruction[118]. The Court took a rights-based approach, as one would expect a constitutional court, forcing a ruling of the judicial authorities, in accordance with Article 11 of the European Charter of Fundamental Rights.

6. CONCLUSION: CO-REGULATION AND CONSTITUTIONALISM

In this article, I assessed the legal definitions and taxonomies of co-regulation, explored the possibility for judicial review of co-regulatory arrangements, and analyzed recent United Kingdom and CJEU case law that concerns human rights and Internet co-regulation. The twelve-point scale that I constructed based on empirical analysis by both a multi-year study for the European Commission, provides further evidence of much earlier stage regulatory intervention by government into forms of governance that had formerly been considered self-regulation. This notably included the funding of 'self-regulatory' organizations as well as the need for incorporation of these arrangements into policy and regulatory Impact Assessments.

Bringing co-regulatory arrangements between government and corporations into the light of judicial review can prove an aid to better regulatory strategy taking into account the multiplicity of 'impure' European co-regulatory forms, whose invisibility from narrower legal positivist analysis needs remedying[119]. It can also lead to exposure of unconstitutional bargains and trade-offs made in the shadows but exposed to the sunlight of regulatory scrutiny[120]. It should lead legal scholars to focus on the balance between efficient regulatory arrangements in economic terms and the need for public oversight of regulation[121], especially in Internet regulation, which is concerned with protection of fundamental human

117 TA No. 81 (2009) Act to promote the dissemination and protection of creation on the Internet ['HADOPI Law'] creating the High Authority for the dissemination of works and protection of rights on the Internet (HADOPI)

118 Conseil Constitutionnel (2009) Decision No. 2009-580 DC of 10 June 2009.

119 For earlier analysis in this vein, see Schulz, W. and T. Held (2004) Regulated Self-Regulation as a Form of Modern Government: A Comparative Analysis with Case Studies from Media and Telecommunications Law, University Of Luton Press; Scott, C. (2005) Between the Old and the New: Innovation in the R egulation of Internet Gaming, in Black, Julia, Martin Lodge and Mark Thatcher (2005) Regulatory Innovation: A Comparative Analysis, Cheltenham: Edward Elgar.

120 See generally Black, J. (1998) Reviewing Regulatory Rules: Responding to hybridisation, in Black, J., P. Muchlinski, P. Walker (eds.) Commercial Regulation and Judicial Review, Hart: Oxford.

121 See Scott's pioneering work on new European governance and the law, in Scott, C. (2004) Regulation in the Age of Governance: The Rise of the Post-regulatory State, in Jordana, Jacint and David Levi-Faur (2004) The Politics of Regulation, Cheltenham: Edward Elgar; Scott, J. and Trubek, D.M. (2002) Mind the Gap: Law and New Approaches to Governance in the European Union, 8 European Law Journal 1.

rights[122]. The United Nations and regional human rights bodies including the OSCE have now recognised the primacy of human rights in Internet regulation[123]. The survey of OSCE countries (56 members total) focussed on Internet filtering law and practice, concluded that data retention, anti-pornography filtering and other techniques are preventing the use of the Internet, which itself should be considered to infringe on users' human rights[124].

It is likely that the shadowy Internet co-regulatory arrangements analyzed will be found insufficiently constitutionally protective of freedom of expression[125]. This raises the prospect of a much more procedurally robust and public exposure of co-regulation to the regulatory gaze. The space within which the European Commission, Member States and corporations have been able to establish their Internet regulation arrangements without significant Parliamentary or judicial interference may be drawing to an end.

122 See Klang, M. & Murray, A. (eds 2004) Human Rights in the Digital Age, Cavendish Publishing, London. A wider global survey is contained in Deibert, R. J., Palfrey, J. G., Rohozinski, R. and Zittrain, J. (eds 2010) Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace, MIT Press, a survey book on Internet access and filtering, documents censorship across countries, accompanied by interactive website at http://www.access-controlled.net/ which also hosts chapters available on an open access basis. It follows previous work published by same authors in project Open Net Initiative, Deibert, R. J., Palfrey, J. G., Rohozinski, R. and Zittrain, J. (eds 2008) Access Denied, Cambridge: MIT Press.

123 See La Rue, Frank (2011) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council Seventeenth session Agenda item 3, A/HRC/17/27 of 17 May 2011 at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

124 See Akdeniz, Yaman (2011) Freedom of Expression on the Internet: Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States, The Office of the Representative on Freedom of the Media, Organization for Security and Co-operation in Europe: Vienna 2011 at http://www.osce.org/fom/80723

125 See McIntyre, TJ (2010) Are Norwich Pharmacal orders compatible with the Data Retention Directive? November 09, 2010, at http://www.tjmcintyre.com/2010/11/are-norwich-pharmacal-orders-compatible.html. McIntyre, TJ, and Scott, C. (2008) Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility' in Brownsword, R and Yeung, K (eds) Regulating Technologies, Oxford: Hart Publishing, at SSRN: http://ssrn.com/abstract=1103030

16

REDEFINIENDO LA *ISEGORÍA*: *OPEN DATA* CIUDADANOS

Helena Nadal Sánchez
Doctoranda del Departamento de Derecho Público de la Universidad de Burgos
Javier de la Cueva González-Cotera
Abogado

RESUMEN: Con las Tecnologías de la Información y Comunicación han aparecido movimientos ciudadanos que extraen, transforman y publican datos públicos, lo que constituye una manera novedosa de aportar información al debate político y de enriquecer la información pública. Esta actividad no es un fenómeno novedoso sino que puede conectarse con el concepto clásico griego de *isegoría* y enmarcarse históricamente en los movimientos que propugnan la transparencia política. Cuando estos movimientos ciudadanos aportan datos, procuran cumplir con los criterios *open data* de la *Sunlight Foundation*, en principio diseñados para ser seguidos por las instituciones públicas. Tras poner como ejemplo cinco supuestos reales de extracción de datos y proponer unos criterios de demarcación para la validez de su transformación y trazabilidad, defendemos que este mecanismo de producción de *open data* por la ciudadanía es igualmente válido que el del Estado. Se produce así la *isegoría* de los datos «tratados por el ciudadano» y de los «tratados por el Estado», lo que constituye bloques básicos de información soporte de la discusión democrática contemporánea, operando la *isegoría* no sólo en el nivel del lenguaje gramatical sino también en el núcleo de los datos tratables mediante las TIC. Como corolario, se apuntan qué aspectos han de cuidarse de los datos abiertos por ser requisitos de la *isegoría* y fundamento de la información soporte de un sistema democrático en el estado actual de la tecnología.

KEYWORDS: *Open data*, *isegoría*, democracia participativa, criterio de demarcación.

1. INTRODUCCIÓN

Constituye un lugar común señalar que la historia es cíclica y se repite. El presente artículo no trata de este aspecto sino que intenta ahondar en conceptos clásicos de la filosofía o del derecho políticos y, jugando con ellos, verificar si tienen aplicación al actual momento caracterizado por una crisis del Estado social y democrático de Derecho. Nos hallamos en una era de inicial desarrollo de las tecnologías de la información y comunicación (TIC), lo que permite que un ciudadano publique a coste cero[1] una información que otros ciudadanos, pertenecientes a cualquier lugar del globo, puedan leerla también a coste cero.[2] Esta capacidad de utilizar un «speakers corner» cuyo eco pueda ser universal, si bien tiene que

1 El coste cero es literal ya que no es difícil el acceso a coste cero de un terminal ajeno, así como la publicación en una plataforma gratuita modelo blogspot o cualquier otra existente.

2 Ver a este respecto la parte inicial de la conferencia *The Aufklärung in the Age of Philosophical Engineering* pronunciada en fecha 20 de abril de 2012 por el filósofo Bernard Stiegler, director del Institut

luchar contra la cacofonía del ruido del entorno, ha demostrado que si la información que conlleva es de una calidad determinada, no puede ser despreciado su aporte a la discusión pública en torno a una política determinada. Los ejemplos ocurridos hasta la fecha son múltiples y variados[3] y no son el objeto de este artículo. De esta manera, la voz de una persona cualquiera puede llegar a tener la misma validez e impacto que la de cualquier grupo organizado público o privado: «the power of one» y «no propongas, haz» se propugnan no como reivindicaciones de la individualidad sino como potencia de la aportación de una persona hacia la comunidad política *online* y como soporte de los fenómenos de masas en Internet.[4]

Ahora bien, Internet como foro político no se limita al uso de oraciones portadoras de ideas a través de las que producir el convencimiento de los votantes para que lleven a cabo una determinada elección, al estilo del *marketing* realizado hasta ahora en mítines, prensa, radio y televisión, ni tampoco se limita a generar contenedores de software que albergan gratuitamente publicaciones (foros y *blogs*) o agregadores de noticias, sino que asistimos a un nuevo fenómeno que es el de la ciudadanía obteniendo datos, transformándolos y publicándolos. No se trata de un ejercicio ni contra el poder ni de control del mismo, sino *praeter legis*, motivado en numerosas ocasiones por un correcto y legítimo entendimiento de la auto gobernanza y para mejorar aquellos aspectos donde otros sistemas de producción o regulación de bienes o servicios son incapaces de llegar. Un ejemplo típico es el de los voluntarios de *Open Street Maps* ante el terremoto de Haití, quienes fueron capaces de generar antes que nadie los mapas luego utilizados por las fuerzas internacionales;[5] otro ejemplo es el de los lectores de *The Guardian* que en junio de 2009 transcribieron el casi millón de documentos que contenían las declaraciones de gastos efectuadas por los miembros del parlamento británico.[6] Parafraseando a FREGE, podemos afirmar que *Internet* no se limita a admitir sólo palabras como argumentos, sino también *objetos de cualquier tipo*.

El presente artículo pretende comenzar una reflexión y línea de investigación sobre el valor de los *objetos de cualquier tipo* presentes en *Internet* rescatando, en el apartado primero, el antiguo concepto de *isegoría* en los datos abiertos creados por los ciudadanos ya que defende-

---

de Recherche et d'Innovation (IRI) del Centre Georges-Pompidou, en el evento World Wide Web Conference 2012: (STIEGLER, 2012).

3 Basta señalar la iniciativa de «Adopte un senador» de la que se hizo eco el diario El País en ejemplar de papel del día 10 de septiembre de 2011y el día anterior en su versión digital. Documento accesible en línea. Fecha de última consulta: 29 de abril de 2012. <http://politica.elpais.com/politica/2011/09/09/actualidad/1315584504_266528.html>

4 Sobre este tema, consúltense las obras: BENKLER, Y. (2006). *The Wealth of Networks. How Social Production Transforms Markets and Freedom*. New Haven y Londres: Yale University Press. Accesible en línea: <http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf> Fecha de última consulta: 29 de abril de 2012. RHEINGOLD, H. (2004). *Multitudes inteligentes.* Barcelona: Gedisa Editorial.

5 Documento accesible en línea: http://haiti.openstreetmap.nl/ Fecha de última consulta: 29 de abril de 2012.

6 Documento accesible en línea: <http://mpsallowances.parliament.uk/mpslordsandoffices/hocallowances/allowances-by-mp/> Fecha de última consulta: 29 de abril de 2012.

mos que lo relevante no sólo es el autor del dato sino la calidad del mismo, lo que genera una nueva base para la esfera pública donde ha de apoyarse el encuentro y construcción democráticos. El conjunto de las opiniones vertidas y de los datos tratados por los ciudadanos, además de formar la *opinión pública* actual, tiene como función la búsqueda de la transparencia de lo político y la facilitación de una mejor gobernanza, lo que supone la continuidad de una larga línea histórica sobre la que hacemos unas breves referencias en el apartado segundo. En el tercer apartado del artículo examinamos los criterios *open data* y señalamos cinco ejemplos reales de extracción de datos, mostrando así directamente el objeto de estudio, y formulamos los criterios de demarcación que han de aplicarse como base de la *isegoría*. Finalizamos el artículo con la reformulación de este concepto habida cuenta que la *opinión pública*, en esta contemporánea nueva Ilustración, ha de hallarse fundada en datos tratables.

2. LA *ISEGORÍA*

La definición aristotélica de la categoría de ciudadano que aparece vinculada a la idea de democracia fue formulada casi a las puertas de su desaparición misma ya que muy poco después, durante el periodo helenístico los griegos dejarían de ser ciudadanos para convertirse en súbditos tras la conquista de Grecia por el imperio alejandrino en el 338 a. C. Para SINCLAIR (1999, 11) esta imagen, casi la última de lo que supuso ser ciudadano en Atenas, representa su culminación como categoría dentro del espacio político de dicha *polis:*

> En el periodo que va desde mediados del siglo V al 322 a. C. Atenas se rigió por medio de un sistema de democracia directa que llevó aparejada la participación de miles de ciudadanos en la Asamblea, los Tribunales y en otras instituciones. El concepto de participación o colaboración es fundamental en el pensamiento y en los textos griegos que tratan sobre la ciudadanía y la vida política. Aristóteles definió como el rasgo más característico de un ciudadano la posesión del derecho a participar en el ejercicio del poder.

La participación en los asuntos públicos llegó a tener una importancia radical para el hecho de ser ciudadano ateniense. Se llegó a establecer un vínculo tal entre ciudadanía y participación que hizo evolucionar la categoría de ciudadano desde una concepción estática característica de la época arcaica hacia una concepción dinámica propia de la democracia. La concepción estática consideraba al ciudadano como poseedor de una serie de derechos y privilegios frente a otros habitantes de Atenas, como los esclavos o los extranjeros y cuyas funciones se limitaban al ámbito de la familia; la concepción dinámica va más allá y dota a la categoría de ciudadano de funcionalidad política. El ideal de la época de Pericles consiste en un hombre comprometido, ante todo ente los negocios de la Ciudad, bien para mandar, bien para obedecer (TOUCHARD: 1987, 31) como queda claramente manifestado en la retórica de Tucídides: «Un hombre puede dedicarse a un tiempo a sus asuntos privados y a los públicos, y los que se vuelcan en sus asuntos no dejan de estar al tanto de la política, pues somos los únicos que no tenemos por inactivo al que no toma parte en nada de esto, sino al inútil» (TUCÍDIDES: 2007, 67)

En este compromiso y en la posibilidad de ejercerlo radica el concepto de *isegoría* del que nos ocupamos en este trabajo. La *isegoría* o igualdad de participación en los asuntos públicos aparece en vínculo con el de *isocracia*, igualdad de participación en el poder, junto

con el de *isonomía* o igualdad de la ley para todos y con el de *isogonía* o igualdad de derechos; todos ellos conforman los fundamentos del Estado democrático griego. En todos aparece el prefijo -iso (igual) que es entendido como la igualdad que hace posible la vida compartida en común y el estado de armonía, una suerte de ley de la naturaleza inherente al hombre que va incluso más allá de la propia polis como describiera EURÍPIDES en las *Fenicias*: «La igualdad, que une a los amigos con los amigos / a las ciudades con las ciudades, a los aliados con los aliados. / La ley de la naturaleza del hombre es la igualdad».

Desde el gobierno de Clistenes (a partir del año 508 a. C.) se había ido produciendo un incremento de participación ciudadana primero en la *Boulé* o Consejo de los Quinientos encargada de supervisar a la *Ekklesía* o Asamblea de la que emanaba la legislación ateniense. Finalmente, durante el gobierno de Efialtes (a partir del 431 a. C.) se produce un acceso universal a los dos órganos por parte de los ciudadanos atenienses (unos 35.000 hacia el año 450[7]) conformando así lo que se dio en llamar el *Demo*.

Nos es desconocido si este derecho de acceso universal a los órganos de gobierno vino dado por un derecho legal o por la costumbre, posiblemente porque la historiografía no parece haber considerado su origen como un hecho relevante. Desde su perspectiva, este derecho de participación ciudadana que se conoció como «*isegoría*» queda reducido exclusivamente al contexto de la Grecia clásica. Pero en un análisis más amplio, donde sea considerado además de como un derecho como una categoría que atraviesa el tiempo y llega hasta nuestras sociedades, entonces el modo como se gesta condiciona su comprensión actual y su proyección futura y en este sentido adquiere capital importancia.

La posición habitual mantenida por la mayor parte de los estudios tiende a considerar que la *isegoría* fue dada por un derecho legal y que por tanto su origen es de carácter político con independencia del momento de su aparición.

Para SINCLAIR, por ejemplo, la apertura a la *isegoría* nace en Atenas a finales de los años 590 a. C. con las reformas del legislador Solón que garantizaron, entre otros, el derecho del pueblo a apelar contra las decisiones de los arcontes o de los funcionarios y con las modificaciones del acceso al poder al acabar con el monopolio de la aristocracia en la ocupación de los cargos públicos (1999, 16). Después de Maratón (490 a. C.) y de Salamina (480 a. C.) se desarrolló un sentimiento de superioridad entre los atenienses que les hacía considerarse no sólo por encima de los persas, sino también por encima del resto de los griegos «porque el orgullo y la confianza no quedaron confinados en un grupo reducido de dirigentes atenienses sino que en los hombres de Maratón y en los marineros de Salamina y en sus hijos -esto es, en el pueblo ateniense en general- existían una conciencia política y un sentimiento de poder crecientes» (1999, 37) y que se manifestó en la seguridad que sentían a la hora de «ser innovadores en la conducción de asuntos públicos» (Ibid.).

GRIFFITH (1966, 117) advierte que es poco probable, por lo temprano, que ya a finales del siglo sexto se diera una participación de la ciudadanía en la asamblea lo suficientemente importante como para hablar de *isegoría*, y sostiene que el derecho a dirigirse a la

7 SINCLAIR (1999, 38).

Asamblea fue mucho más tarde que Solón; más bien lo sitúa propiamente durante las reformas políticas del gobierno de Pericles (461-428 a. C.).

Por otra parte WOODHEAD (1967) defiende la idea según la cual la *isegoría* existía de forma natural y desde siempre en la *Boulé* y que desde ahí se trasladó a la Asamblea aproximadamente a mediados del siglo V con la reformas de este órgano hechas por Clístenes. Para este autor, ya en el periodo arcaico y aunque la aristocracia no formulara principios de *isegoría* como tales, fue una tendencia tácitamente admitida entre los nobles a la hora de dirigirse en los consejos asamblearios como lo fue el Areópago y que de ahí fuera extendiéndose progresivamente a otros órganos a medida que se iban borrando las líneas divisorias entre los ciudadanos. En este sentido existe la posibilidad de que el derecho al acceso universal a los órganos de gobierno se introdujese sin legislación y en ese sentido tuviese un origen en la costumbre.

En la misma línea se sitúa LEWIS, aunque identifica el nacimiento del derecho a hablar en la Asamblea con las reformas de Solón y destaca su marcado carácter político una vez reconocido: cuando Demóstenes (384-322 a.C.) habló de *isegoría* lo hizo identificándola con *isonomía* o igualdad política (1971, 130) y por lo que respecta al testimonio que ofrece Herodoto en su obra (444 a. C.) considera que le dota de un significado claramente político al identificarlo con *isonomía* y con *isocracia* y oponerlo al de tiranía.

Situar el nacimiento de la *isegoría* en el contexto de la costumbre, independientemente de que este contexto fuera el aristocrático, la convierte en una categoría social y en este sentido la universaliza por cuanto abre la posibilidad de entenderla y extenderla en la realidad socio-política actual. En las apuestas de hoy por una participación en los asuntos públicos, independiente de los cauces institucionales, se está construyendo una suerte de *isegoría ciudadana* que se desarrolla al margen del reconocimiento político y que es posiblemente heredera del reconocimiento del otro como igual a la hora de hablar de lo que nos afecta, ya gestada, ya percibida en los principios de la civilización griega. Al igual que en la antigua Grecia en el ámbito del ágora, hoy en día se está produciendo la igualdad de participación en los asuntos públicos en el ámbito de la aportación de las bases informacionales necesarias para construir el espacio político a través de los datos abiertos ciudadanos. Donde antes fue la palabra, hoy son la palabra más los datos estructurados.

3. LA PUBLICIDAD DE LO POLÍTICO

Las aportaciones ciudadanas de datos abiertos tienen como necesidad y como finalidad un régimen de publicidad de lo político: no es algo nuevo que la transparencia en la acción y en las razones de gobierno supongan la legitimidad del mismo. Se trata de una conquista ciudadana que busca ante todo evitar la arbitrariedad del poder y es dentro de este marco conceptual donde tenemos que incluir los nuevos movimientos de datos abiertos tanto estatales como ciudadanos y las reivindicaciones de una ley de transparencia. Para que exista transparencia política, es obvio que ha de existir publicidad y con el fin de señalar las diferentes aproximaciones a estos requisitos citaremos unas breves pinceladas desde la Edad

Moderna que articularemos sobre dos aspectos: la existencia de una información que ha de ser pública y la esfera en la que tal publicidad ha de realizarse.[8]

Comenzaremos haciendo referencia a KANT, quien enumera los beneficios de la publicidad tanto en un aspecto positivo como negativo y en referencia tanto a la relación entre gobernante-gobernados como entre los diferentes Estados. KANT (2008, 61-62) postula como *fórmulas trascendentales* del derecho público las proposiciones negativa de que *«Son injustas todas las acciones que se refieren al derecho de otros hombres cuyos principios no soportan ser publicados» y positiva de que «Todas las máximas que necesitan la publicidad (para no fracasar en sus propósitos) concuerdan con el derecho y la política a la vez» (2008, 69). En lo que se refiere a la publicidad entre los Estados, «el derecho de gentes, como derecho público, implica la publicación de una voluntad general que determine a cada cual lo suyo» (2008, 64).*

La postura kantiana fue explícitamente criticada por SCHMITT (2008, 82), acusándola incluso de ingenuidad y describiendo el funcionamiento del parlamentarismo actual como evidencia contraria no sólo a KANT sino a los demás autores ilustrados que pudieran tener la opinión de que a través de la confrontación de discursos se llega a la verdad o, al menos, a la razón:

> La luz de la publicidad (öffentliche) sería la luz de la Ilustración, la liberación de la superstición, del fanatismo y de las intrigas despóticas. En todos los sistemas donde reina el despotismo ilustrado la opinión pública (öffenliche) desempeña el papel de un correctivo absoluto. [...] la opinión pública (öffenliche) ilustrada haría, de suyo, completamente imposible, cualquier abuso. […] donde reina la libertad de prensa un abuso del poder sería impensable [...] la imprenta es el fundamento de la libertad. (2008, 82).

Para SCHMITT, la realidad es bien diferente: «la publicidad y la discusión se han convertido ... en una formalidad vacua y fútil» habiendo perdido el Parlamento, «tal como se desarrolló en el siglo XIX», «también la base y el sentido que hasta ahora tenía». (2008, 106). Para este autor la publicidad tiene otra función: se trata de un elemento seminal de la representación política. La publicidad no cumple la función instrumental kantiana de transparencia y herramienta ilustradora sino que se trata de uno de los requisitos del Estado. Esto es así porque SCHMITT defiende que «no hay Estado alguno sin representación» (1982, 206) y «la representación no puede tener lugar más que en la esfera de lo público». El lugar de la representación política es el parlamento éste «tiene carácter representativo sólo en tanto que existe la creencia de que su actividad propia está en publicidad» (1982, 208). De sus tesis lógicamente hemos de inferir que si la representación se desarrolla en secreto, sin hallarse en la esfera pública y, por tanto, sin el decorado kantiano de la transparencia, entonces no existirá un Estado sino otra institución, pero no Estado en el sentido moderno. A pesar de lo denostado de este autor, la aportación de SCHMITT tiene el interés de justificar al máximo la necesidad de transparencia y publicidad.

También comentando a KANT, HABERMAS (2006, 136-149) hace referencia a la publicidad como «función de control programático de la verdad» produciéndose durante la época de la Ilustración un proceso de salida a lo público de la opinión antes relegada a los

8 Profundizar en este aspecto excedería de largo los propósitos del presente artículo ya que la transparencia hunde sus raíces en la filosofía desde el inicio de su historia ya que, en definitiva, se trata del problema del ser. Por ello nos conformamos con señalar unas líneas maestras.

ámbitos privados. Para HABERMAS esta salida hoy en día sigue ocurriendo pero en otros órdenes, que son los organizacionales de los partidos políticos y de las asociaciones públicas:

> «la conexión comunicativa de un público raciocinante constituido por personas privadas ha sido cortada; la opinión pública que otrora surgía de esa conexión ha sido en parte descompuesta en opiniones informales de personas privadas sin público, y en parte en opiniones formales de las instituciones publicísticamente activas.» (2006, 272).

En apoyo de que la publicidad está íntimamente ligada con lo político, la obra de ARENDT (1993) supone una referencia necesaria: «ninguna clase de vida humana … resulta posible sin un mundo que directa o indirectamente testifica la presencia de otros seres humanos» (1993, 37). En el sentimiento antiguo, privado significaba «literalmente hallarse desprovisto de algo», no siéndose plenamente humano si no se podía entrar en la esfera pública (1993, 49). Esta última constituye un lugar donde «todo lo que aparece en público puede verlo y oírlo todo el mundo y tiene la más amplia publicidad posible» (1993, 59), un lugar común a todos pero «diferenciado de nuestro lugar poseído privadamente en él» (1993, 61). A estos dos lugares, añade CASTORIADIS (2006b, 21) un tercero, criticando a ARENDT:

> «Siempre hay, de manera abstracta, tres esferas en la vida social considerada desde el punto de vista político. Una esfera privada, la de la vida estrictamente personal de la gente; una esfera pública en la que se toman las decisiones que se aplican obligatoriamente a todos, públicamente sancionadas; y una esfera que puede llamarse público-privada, abierta a todos, pero donde el poder político, aunque es ejercido por la colectividad, no debe intervenir: la esfera donde la gente discute, publica y compra libros, va al teatro, etc. En la jerga contemporánea se han mezclado la esfera privada y la público-privada, sobre todo desde Hannah Arendt»

A través de este brevísimo repaso podemos intuir que la esfera pública, lugar donde se practica la *isegoría*, necesita ser repensado nuevamente. «Desde la perspectiva de un discurso democrático y de una república participativa, la economía de la información de la red ofrece una genuina reorganización de la esfera pública», nos recuerda BENKLER (2006, 465). En esta reorganización deberemos valorar al menos dos aspectos:

- cómo de pública ha de ser esta esfera, para lo que es útil el pensamiento de CASTORIADIS, si la *isegoría* ha de practicarse en la esfera pública o en la pública-privada, esto es, «la esfera donde la gente discute, publica y compra libros, va al teatro», y
- con SCHMITT, dado que «la representación no puede tener lugar más que en la esfera de lo público» los *open data* nucleares de la democracia deben quedar excluidos de ser objeto de «gestión de negocios, cuidado y representación de intereses privados».

4. LA CONSTRUCCIÓN CIUDADANA DE *OPEN DATA*

Ahora bien, ¿cómo construyen los ciudadanos sus datos abiertos y los presentan públicamente? Para responder a esta pregunta, primero recordaremos que tras una reunión celebrada los días 7 y 8 de diciembre de 2007 en Sebastopol, California, sus asistentes[9] redactaron los

9 La relación de los treinta asistentes puede consultarse en línea en https://public.resource.org/open_government_meeting.html Fecha de última consulta: 29 de abril de 2012.

llamados ocho principios de *open data*.[10] Estos principios son los que habían de servir para señalar la manera en que los órganos públicos deben almacenar y poner a disposición pública la información electrónica que se halla en su poder. Con posterioridad, en agosto de 2010, la *Sunlight Foundation* amplió estos principios en dos más,[11] señalándose que el conjunto de los diez constituye un continuo de apertura y su naturaleza es de carácter descriptivo y no normativo, de lo que puede deducirse que los diez apartados corresponden más a criterios que a principios.

Tal y como señalamos en la introducción, en la práctica quienes están liberando *open data* no sólo son los agentes públicos sino también los ciudadanos quienes a través de técnicas de *scraping* (raspado), entre otras, extraen, transforman para cumplir con los criterios *open data* y ponen a disposición pública información que los poderes del Estado han publicado sin cumplir con tales criterios. Este mecanismo de producción de *open data* es igualmente válido que el del Estado, lo que nos llevará a defender una *isegoría* del dato tratado por el ciudadano y el dato tratado por el Estado siempre y cuando los criterios utilizados para su producción sean los de *open data* y cumplan unos determinados requisitos de validez. Se trata de una *isegoría* que opera no en el nivel del lenguaje gramatical sino en el del núcleo de los datos tratables mediante las TIC e implica la equivalencia de la validez de los datos con independencia de quien los trató. Como corolario, esta *isegoría* deviene en el desarrollo de técnicas ciudadanas de control político ejercidas mediante el uso de la tecnología cotidiana.

Para acercarnos mejor a este fenómeno, a continuación mostraremos cinco supuestos diferentes de creación de datos que, sin agotar la diversa problemática ante la que nos enfrentamos, nos permite conocer el objeto de nuestro estudio, objeto al que la ciudadanía le aplica los criterios *open data*, que tomamos de la *Sunlight Foundation* y traducimos a nuestra lengua, proponiendo a continuación un criterio de demarcación para aceptar un conjunto de datos como válido en la construcción de la *isegoría*. En definitiva, se trata de precisar requisitos previos y conceptuales de lo que se ha venido a denominar *e-Government.*

4.1. Supuestos de extracción y generación de datos

Las fases necesarias para la construcción de los datos son (i) la extracción (o generación) de los datos partiendo de unas fuentes, (ii) la transformación de los datos para cumplir los criterios de *open data* y (iii) la publicación de los datos en un repositorio accesible universalmente. Estas tres fases son comunes a cualquier persona pública o privada que desee generar unos datos que puedan subsumirse bajo el concepto de *open data*.

La casuística con la que nos hallamos en la práctica es muy variada, por lo que previamente a cualquier formulación de hipótesis, es conveniente analizar cinco supuestos de construcción de *datos abiertos* ciudadanos. Cada supuesto tiene una peculiaridad, por lo

10 Documento accesible en línea: http://www.opengovdata.org/home/8principles Fecha de última consulta: 29 de abril de 2012.

11 Documento accesible en línea: http://sunlightfoundation.com/policy/documents/ten-open-data-principles/ Fecha de última consulta: 29 de abril de 2012.

que esta muestra sirve para orientarse por la diferente problemática ante la que se enfrenta el tratamiento de datos e intentar formular reglas generales. Ha de advertirse que con estos cinco supuestos no se agota la diversidad en la generación de datos. En todos los supuestos partimos de unas fuentes públicas accesibles al público como lo pueden ser los diversos boletines oficiales o webs de organismos institucionales.

1. Presidentes de la Comunidad Autónoma de Cantabria

Los nombramientos de los presidentes de las comunidades autónomas se publican en el Boletín Oficial del Estado por lo que para construir una lista de presidentes de la comunidad autónoma cántabra bastaría una búsqueda en la página web de dicho boletín. Sin embargo, dado que el título de «Comunidad Autónoma de Cantabria» antes fue el de «Diputación de Cantabria» obtendríamos resultados incompletos. La creación de esta lista no puede hacerse mediante una búsqueda en el Boletín Oficial del Estado sin previamente tener un conocimiento de estos hechos históricos. Ello implica que para automatizar la búsqueda mediante un *script* se requiere incluir en el mismo dos variables del título en la búsqueda. Dado el mínimo número de presidentes, es más costoso crear un *script* que realizar una consulta y extracción manuales.[12]

2. Ordenes ministeriales

La construcción de un listado de las órdenes ministeriales se realiza mediante la búsqueda de la categoría «orden ministerial» en la página *web* del Boletín Oficial del Estado. El problema en este caso consiste en no poder conocer si los resultados del BOE arrojan todas las órdenes ministeriales. Para resolver este problema ha de conocerse que las normas jurídicas se numeran, por lo que habrá de verificarse que la numeración sea continua.[13] Sin embargo, no puede garantizarse que al final de cada año no se hayan omitido normas.

3. Reales decretos legislativos

Al igual que los datos sobre órdenes ministeriales, se obtiene mediante la búsqueda de la categoría «Real decreto legislativo» en la página web del Boletín Oficial del Estado. Ocurre la misma problemática anterior sobre si los datos son completos, pero dado que los reales decretos legislativos tienen una tramitación parlamentaria, pueden cuadrarse los datos extraídos de las *webs* del Congreso de los Diputados y del Senado. La multiplicidad de fuentes permite una mayor garantía de corrección de los datos.[14]

---

12 https://docs.google.com/spreadsheet/ccc?key=0AtDiDXlt-a__dFVZVGJtZ3hOZ1hnRWdnNVB3cFYtR3c&hl=es#gid=0 Fecha de última consulta: 29 de abril de 2012.

13 Documento accesible en línea: https://docs.google.com/spreadsheet/ccc?key=0AtDiDXlt-a__dGhfTzZ5UDFLZ3JxNlJlNFAtY3oyaHc&hl=es#gid=0 Fecha de última consulta: 29 de abril de 2012.

14 Documento accesible en línea: https://docs.google.com/spreadsheet/ccc?key=0AtDiDXlt-a__dGxSdTJrSjlkRUVCcVNyUkxiS2VXTHc&hl=es#gid=0 Fecha de última consulta: 29 de abril de 2012.

4. Diputados del Congreso

Esta lista[15] se ha obtenido mediante técnicas de *scraping* (raspado) en la *web* del Congreso de los Diputados. El *script* para la extracción de datos[16] está en software libre (es código abierto), lo que permite repetir el raspado y verificar si los resultados obtenidos coinciden.

5. Organos constitucionales

Se obtiene leyendo la Constitución española y extrayendo de ella los órganos constitucionales. La metodología es puramente jurídica, dado que lo que es un órgano constitucional pertenece al ámbito del Derecho constitucional.[17]

En los cinco supuestos, además de la problemática propia de cada uno de ellos, podemos encontrarnos con que las fuentes originarias se desconecten de Internet, cambien sus URL o la información original que contienen las páginas. Queda sin resolver, asimismo, la corrección unilateral de los datos por parte de la institución pública con ocasión de errores detectados o por otros propósitos ilegítimos y que plantearía la necesidad de la realización de una réplica exacta de lo publicado en las webs oficiales por parte de la ciudadanía.[18]

4.2. Los criterios *open data*

Transcribimos a continuación los criterios[19] señalados por la *Sunlight Foundation* dada la relevancia de los mismos en el mundo del activismo *open data*. Supone la guía por la que se rigen todas las aportaciones ciudadanas a los datos abiertos:

Datos completos

> Los datos puestos a disposición pública por el gobierno deben ser lo más completos posibles, reflejando lo que se halla archivado sobre un tema concreto. Deberá ponerse a disposición pública toda la información en bruto, con la excepción de los datos sobre privacidad según lo obligado por las leyes. Los metadatos que definen y explican los datos en bruto deberán estar incluidos, junto con las fórmulas y explicaciones de cómo se han calculado los datos. De esta manera se permite a los usuarios de la información comprender el alcance de la información y examinar cada dato con el mayor nivel de detalle.

---

15 Documento accesible en línea: https://docs.google.com/spreadsheet/ccc?key=0AtDiDXlt-a__dFRXeGo0d28wLUpqMHl1VlA5S3c5Umc&hl=es#gid=0 Fecha de última consulta: 29 de abril de 2012.

16 Documento accesible en línea: https://raw.github.com/gist/1129616/c47caef8d4b94235164b3bd7a4cbb671eec0b750/congreso_twitter.py Fecha de última consulta: 29 de abril de 2012.

17 Documento accesible en línea: https://docs.google.com/spreadsheet/ccc?key=0AtDiDXlt-a__dHEteklITjFJWGFPdmUyRUVwOVF0c3c&hl=es#gid=0 Fecha de última consulta: 29 de abril de 2012.

18 Se trataría de *web* modelo cuyo modelo es http://archive.org pero de todas las *webs* oficiales de un Estado.

19 Documento accesible en línea: http://sunlightfoundation.com/policy/documents/ten-open-data-principles/ Fecha de última consulta: 29 de abril de 2012.

Primariedad

Los datos puestos a disposición pública por el gobierno deben ser de fuentes primarias. Esto incluye la información original recolectada por el gobierno, detalles de cómo se recolectó la información y los documentos fuentes originales. La difusión pública permitirá a los usuarios verificar que la información fue recogida de una manera adecuada y exacta.

Oportunidad

Los datos puestos a disposición pública por el gobierno deben ponerse a disposición pública de manera que sean oportunos. Siempre que sea posible, la información recogida por el gobierno deberá ser puesta a disposición tan rápidamente como es reunida y recogida. Deberá darse prioridad a los datos cuya utilidad es sensible al tiempo. Las actualizaciones en tiempo real maximizarían la utilidad que el público puede obtener de esta información.

Facilidad de acceso físico y electrónico

Los conjuntos de datos publicados por el gobierno deberán ser lo más accesibles posible, definiéndose la accesibilidad como la facilidad con la que se puede obtener dicha información, ya sea a través de medios físicos o electrónicos. Las barreras para el acceso físico incluyen los requisitos de visitar personalmente una oficina o cumplir con requisitos determinados (como, por ejemplo, rellenar formularios o enviar solicitudes en virtud de la FOIA).[20] Las barreras para el acceso electrónico automatizado incluyen hacer accesible los datos a través únicamente previa presentación de formularios o a través de sistemas que requieran navegadores orientados a tecnologías (por ejemplo, Flash, JavaScript, cookies y applets Java). Por el contrario, los datos son mucho más accesibles cuando se proporciona a los usuarios una interfaz para descargar de una sola vez toda la información almacenada en una base (conocido como acceso «a granel») y los medios para hacer llamadas específicas de datos a través de una interfaz de programación de aplicaciones (API). (Uno de los aspectos de este principio es la capacidad de localizar fácilmente y descargar el contenido).

Lectura por máquinas

Las máquinas pueden manejar ciertos tipos de entrada de información mucho mejor que otros. Por ejemplo, las notas manuscritas en papel son muy difíciles de procesar por las máquinas. Escanear texto a través de sistemas de reconocimiento óptico de caracteres (OCR) da lugar a muchos errores de coincidencia de caracteres y de formato.

20 *FOIA request*: Petición de entrega de información pública realizada en ejercicio de los derechos contenidos en la *Freedom of Information Act* (ley de libertad de información).

La información compartida en el ampliamente utilizado formato PDF es muy difícil de analizar por las máquinas. Por tanto, la información debe ser almacenada en formatos que, ampliamente utilizados, permitan el procesamiento por máquinas. (Cuando haya otros factores que hagan necesario el uso de formatos difíciles de analizar, los datos también deberán estar disponibles en formatos de fácil tratamiento). Estos archivos deberán ir acompañados por la documentación relacionada con el formato y su forma de uso en relación a los datos.

No discriminación

La no discriminación hace referencia a quién puede acceder a la información y cómo deben hacer el acceso. Las barreras al uso de los datos pueden incluir registro o requisitos de ser socios. Otra barrera es el uso de «jardines amurallados», que consiste en que sólo se les permite el acceso a algunas aplicaciones. En su forma más amplia, el acceso sin discriminación a los datos significa que cualquier persona puede acceder a los datos en cualquier momento sin necesidad de identificarse o dar ninguna justificación por realizar dicho acceso.

Utilización de estándares abiertos

Los estándares de propiedad común (o estándares abiertos) hacen referencia a quién es el propietario del formato en el que los datos se hallan almacenados. Por ejemplo, si sólo una empresa fabrica el programa que puede leer un archivo en el que los datos se hallan almacenados, el acceso a la información dependerá de usar el programa de procesamiento de dicha empresa. En ocasiones tal programa no es accesible para el público bajo ningún coste o, si es accesible, lo es mediante el pago de una suma. Por ejemplo, Microsoft Excel es un programa de hoja de cálculo de uso bastante extendido cuyo uso cuesta dinero. Existen formatos alternativos libremente disponibles mediante los cuales la información archivada puede ser accedida sin necesidad de una licencia de software. Remover este coste permite que la información pueda ser potencialmente alcanzada por un mayor número de usuarios.

Licencia

La imposición de condiciones legales, requisitos de atribución de autoría, restricciones de difusión y demás ejemplos actúa como barreras para el uso público de los datos. La apertura máxima incluye etiquetar claramente la información pública como una obra del gobierno, accesible sin restricciones y utilizable como parte del dominio público.

Permanencia

La permanencia es la capacidad de encontrar información a través del tiempo. La información divulgada por el gobierno debiera ser «pegajosa», esto es, accesible a perpetuidad mediante archivos en línea. En ocasiones, la información se actualiza, se cambia

o se borra sin ninguna indicación que se ha realizado una alteración. O se pone a disposición como un flujo de información que no se archiva. Para su mejor uso por el público, la información que se pone a disposición en línea debería permanecer en línea, con un adecuado seguimiento temporal de las versiones y archivos.

Costes de uso

Una de las mayores barreras de acceso a una información ostensiblemente accesible es el coste impuesto para el acceso público incluso cuando dicho coste es mínimo. Los gobiernos utilizan una serie de bases para cargar al público el acceso de sus propios documentos: el coste de crear la información, una base de recuperación del coste (coste de producir la información dividido por el número esperado de compradores), el coste de obtener la información, coste por página y por requerimiento de información, coste de procesamiento, coste de duplicación, etcétera. La mayor parte de la información gubernamental se recolecta para propósitos de gobierno y la existencia de precios para los usuarios tiene poco o ningún efecto en si el gobierno recolecta los datos. Imponer precios para el acceso sesga el conjunto de quién está deseando (o quién es capaz) de acceder a la información. También puede impedir usos transformativos de los datos que a su vez pudieran tener como retorno un crecimiento económico e ingresos por impuestos.

4.3. Criterios de demarcación para determinar la validez del dato

Para finalizar con nuestros criterios para la predicabilidad de la *isegoría*, es consustancial a la creación de *open data* ciudadanos que los mismos puedan ser sometidos a criterios de demarcación de su validez, esto es, que sea posible demostrar la objetividad y coherencia de los datos incorporados (siendo esencial la trazabilidad de los mismos) como la validez de los datos que genera. Solo de esta manera estaremos en condiciones de proponer una verdadera *isegoría* a partir de la puesta a disposición de la ciudadanía de datos tratables para su análisis e interpretación.

Nótese que estamos hablando en términos de *validez*[21] y no de *verdad*. La validez es la propiedad correspondiente a la corrección formal de una serie de premisas, es decir, a una vinculación adecuada o concordancia de las mismas, sin inclusión de elementos que no se hallen ya en los propios axiomas o postulados iniciales, mientras que la verdad es siempre una propiedad en conexión con los datos de la experiencia. Consideramos aquí que las únicas instancias que encarnan esta propiedad son las fuentes oficiales a las que hemos identificado como dichos axiomas o postulados iniciales y desde los mismos habrá de asegurarse la correcta trazabilidad de todo dato derivado. Tenemos pues, por una parte, la validez formal que garantiza la limpieza de la trazabilidad del dato en aras a su posterior utilización por parte de la ciudadanía y por otra la verdad empírica, que no entramos a valorar y que atribuimos a las fuentes oficiales.

21 Respecto a la distinción entre validez y verdad consúltese: GARCÍA. 2008, 221-238.

Identificada pues la necesidad de establecer este tipo de criterios de demarcación de la validez de la trazabilidad del dato en los procesos de *open data* ciudadanos, hemos construido una primera propuesta de lenguaje formal axiomático con forma de cálculo[22] que exprese con mayor exactitud las relaciones entre los objetos que estamos tratando y que nos asegure la coherencia en el paso de unos enunciados a otros, siendo tales enunciados el conjunto de datos tratados por los ciudadanos y garantizándose así que cuando un dato se mueve de un formato a otro o se obtiene de la combinación de otros dos o más datos, pueda comprobarse la corrección de la operación.

El cálculo tomaría la siguiente forma:

1. Un conjunto de signos primitivos o alfabeto que pueden ser de dos tipos:
   a. Constantes: conceptos o categorías que subsumen series de variables. Por ejemplo para nuestra propuesta, «órgano constitucional», «nombre», «apellidos.
   b. Variables: Datos obtenidos mediante sistemas de extracción a partir de fuentes oficiales. Por ejemplo «Congreso de los Diputados», «Alicia», «López López».
2. Un repertorio de reglas de extracción de datos que definen qué conceptos y qué variables forman parte del sistema o dicho de otro modo, que son susceptibles de extracción para su posterior tratamiento y deben cumplir la propiedad lógica de la *decidibilidad* es decir para toda fórmula del lenguaje, en este caso para todo dato, puede averiguarse, en un número finito de pasos si es extraíble a partir de los postulados básicos.
3. Una relación de axiomas que son los postulados primeros e indiscutibles del sistema y que para este caso consideramos las *webs* oficiales del Estado (Boletín Oficial del Estado, boletines de las comunidades autónomas y de la administración local) y las *webs* institucionales.
4. Las reglas de transformación que permitan una trazabilidad válida o coherente de los datos desde un formato electrónico no tratable a otro sí tratable y desde un orden categorial determinado a otro u otros esencialmente distintos y todo ello con el objetivo de su puesta a disposición de la ciudadanía. Estas reglas se concretan o bien en un programa informático (*script*) o bien en un procedimiento manual.

La anterior propuesta de cálculo incluye los elementos que constituyen todo el proceso de *open data* ciudadanos hasta constituir un todo interdependiente en forma de la ya mencionada secuencia de extracción (o construcción), transformación y publicación de los datos en un repositorio accesible universalmente.

El criterio último de demarcación de la validez de la trazabilidad del dato vendrá dado por la posibilidad de acceso al código (los *scripts*) que ha generado la reglas de inferencia. Los *scripts* que se utilizan para la tarea de raspado (*scraping*) de las webs oficiales han de ser de código abierto para poder verificar su funcionamiento y comprobar que el dato resultante ha sido obtenido mediante un proceso de transformación en coherencia con las fuentes de

22 Para la noción de cálculo, consúltese: DEAÑO. 2009, 28-45; FALGUERA y MARTÍNEZ. 1999, 57-65.

datos originarias, a las que hemos considerado axiomas y de las que se presupone su verdad empírica.

Si bien podría objetarse que no nos hemos movido de un nivel meramente sintáctico/semántico[23] sin embargo la evidente consecuencia del modelo es su asociación con una pragmática,[24] esto es, con el uso que pueda hacer la ciudadanía de los datos extraídos, transformados y puestos a su disposición una vez confirmada su validez. Esta asociación entre la pragmática y los criterios de validez sintáctico/semánticos constituye específicamente el fundamento último del actual sentido del concepto de *isegoría* en cuanto que en virtud de ella los ciudadanos pueden disponer de otras fuentes de datos de carácter público que, siendo igual de fiables que las fuentes oficiales, les permitan un análisis de la información desde parámetros propios y la programación de acciones efectivas en favor de un nuevo paradigma de participación en los asuntos públicos.

4. LA *ISEGORÍA*, REFORMULADA

Si en la *polis* «todo el mundo tiene algo que decir sobre la ley» (CASTORIADIS, 2006a, 69), hoy todos tenemos algo que decir sobre los datos abiertos. La política, continúa diciendo este autor, nace cuando «la colectividad decide hacerse cargo de sus asuntos y no solamente de sus asuntos cotidianos sino de aquello que en lenguaje corriente se denomina legislación, es decir, finalmente su institución». La reformulación en el contexto tecnológico actual del concepto de *isegoría*, lo tomemos en su sentido de igualdad de participación en los asuntos públicos o en el sentido de *isonomía*, implica tomar como iguales los *open data* con independencia de su origen y siempre y cuando se cumplan tanto los criterios señalados por la *Sunlight Foundation* como los de demarcación para su validez. Según afirmamos en el apartado anterior, si la democracia se fundamentaba sobre la palabra cuya utilización y transmisión se realizaba en el ágora, en la actualidad a la palabra se le añaden los datos, bien sean tratados por el Estado o por los particulares, cuya utilización y transmisión se realiza en las redes de telecomunicaciones. Quién sea el sujeto que trate los datos puede implicar una redistribución del poder en una sociedad.

Para la existencia de un debate que sea el soporte de la democracia se plantea, por tanto, una triple cuestión: una liberación de los formatos, una no restricción por las normas jurídicas y un sometimiento a unos criterios formales.

La liberación de los formatos implica el sometimiento de los datos públicos a estándares abiertos obligatorios, lo que es un aspecto fácilmente aplicable si bien choca con el problema de la presión de los *lobbies* a quienes les interesa imponer los formatos propietarios. Someter los datos a formatos propietarios implica someter los elementos base de la opinión pública a una posibilidad de control por parte del titular jurídico del formato que para tratar

23 Para una comprensión global de la relación sintaxis/semántica véase: ACERO (ed.). 2007.

24 Para una comprensión global de la pragmática lingüística véase: DASCAL. 1998.

los datos nos obligaría a utilizar su software que podría cerrar unilateralmente (si no estuviese ya cerrado, lo que es el caso de Microsoft).

Más relevante para nuestro análisis es la no restricción (o liberación) jurídica de los datos abiertos núcleo de la democracia, bien se utilicen éstos con el propósito ilustrado de la obtención de una mejor razón (KANT), bien para que la representación política no sea falsa (SCHMITT). Esta liberación supone dos dimensiones: la del espacio en el que se usan los datos y la de la normativa jurídica a la que éstos se someten.

En cuanto al espacio en el que se utilizan los datos, éstos pueden usarse tanto en un *topos* público frente al privado (ARENDT) o en uno público frente al privado o el público-privado (CASTORIADIS), por lo que deberán articularse los sistemas para que el *topos* no impida la obtención, transformación y distribución entre otras medidas mediante la apertura de las APIS[25] (DE LA CUEVA, 2008, 173).

No parece adecuada la actual regulación de propiedad intelectual o reutilización de la información del sector público.

- La primera de las regulaciones, la propiedad intelectual, se caracteriza por un *todo lo que no está permitido está prohibido*, lo que paradójicamente es un principio de derecho de los Estados totalitarios y justo lo contrario que debe realizarse con la información núcleo de la democracia, que tiene que estar sometida a los criterios de la libertad de expresión y derecho a la información. No es de recibo que los derechos fundamentales de expresión y derecho a la información puedan verse limitados por un derecho de jerarquía ordinaria como los derechos de autor: la dimensión política de los *open data* no debe hallarse sometida a un derecho que regula jerarquías muy inferiores a las normas instituyentes de una comunidad.
- Tampoco parece muy adecuada la normativa de reutilización de la información del sector público, al menos para un núcleo duro de los datos públicos. Pretender que los datos abiertos, núcleo de una mejor razón o de una transparencia en la representación, puedan ser objeto de comercio se nos hace muy obsceno.

En definitiva, y frente a las tendencias actuales, se trataría de repensar si los *open data* han de tratarse como una *res extra commercium,* si debe existir un núcleo duro de los mismos que por su propia vinculación con la representación política no debe ver limitado su tratamiento informacional y si son adecuadas las categorías jurídicas de la propiedad intelectual o de la reutilización de la información del sector público como marcos legales.

Por último, el sometimiento del tratamiento de los *open data* a unos criterios formales permite el intento de devolver la seriedad y el rigor a un mundo político cuyos gobernantes tratan la información peor que sus administrados, siendo éstos quienes aportan las guías de las que carecen sus representantes políticos. El camino a la *isegoría* se abre nuevamente a través

25 API: *Application programming interface*. Una API es una interfaz visible en Internet de una aplicación que se ejecuta en un servidor. Otro ordenador puede hacer una llamada a esa API pidiendo datos. Señalamos analógicamente y con ánimo pedagógico que las APIs cumplen la misma función entre ordenadores que las sinapsis entre neuronas.

de la mejor eficacia en el tratamiento informacional del *open data* que como bien sabemos por estar presenciándolo, en la actualidad no está en manos de los dirigentes sino de los dirigidos.

5. BIBLIOGRAFÍA

Acero J. J. (ed.) (2007). *Filosofía del lenguaje I. Semántica*, Madrid: Editorial Trotta.

Alonso, J. M., Ambur, O., Amutio M. A., Azañón, O., Bennett, D., Flagg, R., Mcallister, D., Novak, K., Rush, S., Sheridan, J. (2009). *Improving Access to Government through Better Use of the Web*. W3C Interest Group Note 12 May 2009. Accesible en línea. Fecha de última consulta: 22 de abril de 2012. http://www.w3.org/TR/egov-improving/

Arendt, H. (1993). *La condición humana*. Barcelona: Paidós.

Belhajjame, K., Cheney, J., Garijo, D., Lebo, T., Soiland-Reyes, S., Zednik, S. (2011) *The PROV Ontology: Model and Formal Semantics*. W3C Working Draft 13 December 2011. Accesible en línea. Fecha de última consulta: 22 de abril de 2012. http://www.w3.org/TR/2011/WD-prov-o-20111213/

Benkler, Yochai (2006). *The Wealth of Networks. How Social Production Transforms Markets and Freedom*. New Haven y Londres: Yale University Press. Accesible en línea: <http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf> Fecha de última consulta: 29 de abril de 2012.

Bennet, D., Harvey, A. (2009). *Publishing Open Government Data* . W3C Working Draft 8 September 2009. Accesible en línea. Fecha de última consulta: 22 de abril de 2012. http://www.w3.org/TR/gov-data/

Berners-Lee, T. (2009) *Putting Government Data Online*. Accesible en línea. Fecha de última consulta: 22 de abril de 2012. <http://www.w3.org/DesignIssues/GovData.html>

Castoriadis, C. (2006a). *Lo que hace a Grecia. 1. De Homero a Heráclito. Seminarios 1982-1983. La Creación humana II*. México: Fondo de Cultura Económica.

— (2006b). *Una sociedad a la deriva*. Buenos Aires: Katz.

De La Cueva, J. (2008). Derecho y Tecnología: la apertura de las APIS, en *Propiedad Intelectual. Nuevas tecnologías y libre acceso a la cultura*, Universidad de las Américas, Puebla, México, pp. 173–185. Accesible en línea. Fecha de última consulta: 29 de abril de 2012. http://www.ccemx.org/img_act_x_tipo/propiedadint.pdf

Dascal, M. (1998). *Filosofía del lenguaje II. Pragmática*. Madrid: Editorial Trotta.

Deaño, A. (2009). *Introducción a la lógica formal.* Madrid: Editorial Alianza.

Eurípides (1998). *Helena, Fenicias, Orestes, Ifigenia en Aulide*. Madrid: Editorial Gredos.

Falguera, J. L. y Martínez Vidal, C. (1999). *Lógica clásica de primer orden.* Madrid: Editorial Trotta.

García, C. (2008). *El arte de la lógica.* Madrid: Editorial Tecnos, 2008.

Griffith, G. T. (1966). «Isegoria in the Assembly of Athens». En *Ancient Society and Institutions*. (Oxford 1966), pp. 115-138.

Habermas, J. (2006) *Historia y crítica de la opinión pública. La transformación estructural de la vida pública*. Barcelona: Editorial Gustavo Gili.

Kant, I. (2008). *Sobre la paz perpetua* (7ª ed.). Madrid: Editorial Tecnos.

Lewis, J. D. (1971). «Isegoria at Athens: When Did It Begin?». En *Historia: Zeitschrift für Alte Geschichte,* Bd. 20, H. 2/3 (2nd Qtr., 1971) pp. 129-140. Documento accesible en línea. Fecha de última consulta: 29 de abril de 2012. http://www.jstor.org/stable/4435186.

Schmitt, C. (2008). *Los fundamentos histórico-espirituales del parlamentarismo en su situación actual.* Madrid: Editorial Tecnos.

— (1982). *Teoría de la Constitución*. Madrid: Alianza Editorial.

Sinclair, R. K. (1999). *Democracia y participación en Atenas*. Madrid: Editorial Alianza.

Stiegler, B. (2012). *The Aufklärung in the Age of Philosophical Engineering* . Documento accesible en línea. Fecha de última consulta: 21 de abril de 2012. <http://www2012.wwwconference.org/documents/Stiegler-www2012-keynote.pdf>

Touchard, J. (2008). *Historia de las ideas políticas*. Madrid: Editorial Tecnos.

Tucídides (2007). *El discurso fúnebre de Pericles*. Madrid: Editorial Sequitur.

Woodhead, A. G. (1967). «ISEGORIA and the Council of 500». En *Historia*, 16 (1967), pp. 129-140.

CONSTITUCIÓN 2.0 Y ESTADO DE E-DERECHO: A PROPÓSITO DEL PROCESO CONSTITUYENTE ISLANDÉS

Pere Simón Castellano
Becario de investigación (BR) de Derecho Constitucional;
Investigador de la Cátedra de Cultura Jurídica de la Universidad de Girona

RESUMEN: Uno de los ideales más apreciados en el debate internacional en el campo del derecho es el imperio de la Ley. Este concepto, que históricamente se ha vinculado a los valores democráticos y a la máxima legal que indica que nadie está por encima de la ley, evoluciona a la par de las transformaciones sociales. La globalización y la revolución tecnológica están cambiando algunos de los paradigmas que tradicionalmente se han asociado a las nociones de soberanía, imperio de la Ley, Estado de Derecho y Constitución, que están interrelacionadas. Más concretamente, en este trabajo se estudian algunos principios relacionados con el Estado Democrático, como son la transparencia o publicidad de la actuación de los poderes estatales y la participación de la ciudadanía en los asuntos públicos y en los procedimientos legislativos, que cobran un nuevo sentido gracias al empleo de las Tecnologías de la Información y la Comunicación (en adelante, TICs). El autor focaliza así su análisis en el factor tecnológico y en las ingentes posibilidades que este incorpora, poniendo como modelo el proceso constituyente 2.0 islandés, que ejemplifica como las TICs pueden contribuir notablemente a la eficacia del imperio de la Ley y de los demás principios constitucionales que están relacionados.

PALABRAS CLAVE: Constitución 2.0, imperio de la Ley, gobierno abierto u «open Government», democracia deliberativa, TICs, participación.

1. A MODO DE INTRODUCCIÓN: IMPERIO DE LA LEY Y ESTADO DE DERECHO EN EL UNIVERSO 2.0

La posición que la ley ocupa en los ordenamientos jurídicos de los estados democráticos, a pesar de responder a esquemas distintos según la base política de cada país y la construcción dogmática que se construya en base al texto constitucional en cuestión, muestra por lo general rasgos comunes en todos los países de tradición liberal[1]. Esto responde, en gran medida, a la vigencia de algunas ideas ilustradas y principios decimonónicos que el constitucionalismo europeo se esforzó en defender; todos ellos relacionados con la idea de someter a los poderes del Estado –legislativo, ejecutivo y judicial– a la Ley, garantizando la supremacía de la segunda sobre los primeros. Hacemos referencia al principio francés del imperio de la Ley como expresión de la voluntad popular, a la doctrina inglesa del *rule of law*

1 Véase sobre esta cuestión De Otto y Pardo, I. (1987). Derecho constitucional: Sistema de fuentes. En Ignacio de Otto y Pardo (2010), *Obras completas* (p. 803-1088). Oviedo: Universidad de Oviedo/ Centro de Estudios Políticos y Constitucionales. En concreto, véanse las p. 923 y ss.

y a la construcción alemana del *Rechtsstaat* o Estado de Derecho. En cualquiera de esos tres casos, el Estado constitucional aparece como garantía de la primacía de la Ley frente a las demás fuentes del derecho, o lo que es lo mismo, un Estado que tiene sus cimientos en una estructura interna en la que se observa la regla de la primacía de la Ley.

Con todo, y como decía anteriormente, las constituciones de los Estados democráticos recogen por lo general el principio del imperio de la Ley como un ideal que legitima el sistema y el ejercicio de los poderes. Sin ir más lejos, en el Preámbulo de la Constitución Española de 1978 (en adelante, CE) se dice que «la Nación Española […] proclama su voluntad de consolidar un Estado de Derecho que asegure el imperio de la Ley como expresión de la voluntad popular». Tal principio general se concreta en el principio de legalidad –art. 9.3 CE–; en el ejercicio de la función ejecutiva y la potestad reglamentaria «de acuerdo con la Constitución y las leyes» –art. 97 CE–; en la actuación de la Administración Pública «con pleno sometimiento a la ley y al Derecho» –art. 103.1 CE–; en el control judicial de la potestad reglamentaria y la legalidad de la actuación administrativa –art. 106.1 CE–; en el sometimiento de los jueces y magistrados al imperio de la Ley –art. 117.1 CE–.

Este ideal ha sido tradicionalmente asociado a otros apreciados principios, como son el Estado de Derecho, la rendición de cuentas, la separación de los poderes estatales y el sometimiento de estos a la Ley[2]. Así, se entiende que la legitimación de los poderes estatales se produce mediante la Constitución, que traduce la voluntad del pueblo, que es soberano, en ley. Luego no es de extrañar que algunos autores definan el imperio de la Ley como el ideal que pretende que «any exercise of power must be interpretable as emanating from a constitutional provision»[3]. En las democracias constitucionales todos los poderes estatales emanan de la Constitución, que recoge el mandato del pueblo soberano. Y mediante la expresión de esa voluntad soberana del pueblo el Estado democrático alcanza legitimidad. Luego puede afirmarse que la legitimidad de los poderes estatales en una sociedad democrática descansa esencialmente en la voluntad de la ciudadanía, que se expresa directamente o a través de representantes. Tal idea se refleja claramente en el aforismo: «in free governments, the rulers are the servants, and the people their superiors and sovereigns»[4]. O en las palabras: «I am a Citizen of a Country which knows no other Majesty than that of the People […] no other Sovereignty than that of the Laws»[5].

Sin embargo, tales afirmaciones no encajan del todo con lo que a la praxis ha significado el principio del imperio de la Ley, en gran parte debido a las dificultades prácticas para permitir el ejercicio real de la soberanía por parte del pueblo, garantizar la participación de

2 Vid. por todos Chevallier, J. (1994). *L'Etat de droit*. Paris: Montchrestien.

3 De Hert, P. y Gutwirth, S. (2006). Privacy, data protection and law enforcement: Opacity of the individual and transparency of the power. En Erik Claes, Antony Duff y Serge Gutwirth (eds.), *Privacy and the Criminal Law* (p. 61-104). Antwerpen–Oxford: Intersentia, p. 65.

4 Las palabras se atribuyen a Benjamin Franklin. Recuperado en 23 de marzo de 2012, en http://bit.ly/vWsT5k

5 Paine, T. (1995). To the Authors of *The Republican*. En Eric Foner (ed.), *Collected Writings* (p. 376). New York: Library of America.

los ciudadanos en la gestión de los asuntos públicos y acabar con la opacidad de los poderes. La participación de los ciudadanos en la cosa pública se ha canalizado tradicionalmente a través de las elecciones democráticas periódicas –democracia representativa–, mientras que el control de los poderes estatales ha quedado a manos de una opinión pública que, en un primer momento representaba tan solo las opiniones de un público más que reducido[6], y posteriormente, a pesar de que este se amplió considerablemente, pasó a estar fuertemente influenciado o condicionado por los *mass media*[7].

Buena muestra de que la teoría no siempre coincide con la realidad puede encontrar-se en algunos estudios recientes que han intentado ofrecer una imagen completa y detallada de la situación actual, por lo que a eficacia se refiere, del imperio de la Ley[8]. En concreto, en el estudio *Rule of Law Index 2011*, realizado en el marco del *The World Justice Project*, se han estudiado nueve factores o dimensiones vinculados al citado principio: la limitación de los poderes gubernamentales, la ausencia de corrupción, el orden y la seguridad, el reconocimiento y la tutela de los derechos fundamentales, el gobierno abierto, la aplicación efectiva del Derecho, el acceso a la justicia civil, la efectividad de la justicia penal y, por último, la justicia «informal» o la existencia de sistemas alternativos de resolución de conflictos. Todas estas dimensiones teóricas se desglosan a su vez en una serie de preguntas precisas y delimitadas que permiten evaluar la efectividad del imperio de la Ley mediante las respuestas que ciudadanos y expertos de los países consultados ofrecen. En otras palabras, se vinculan definiciones conceptuales teóricas con cuestiones concretas y se estudia la vigencia del Estado de Derecho país por país.

En este contexto, y teniendo en cuenta que las premisas teóricas que se derivan del principio del imperio de la Ley pueden traducirse a la práctica en un conjunto de cuestiones concretas, tiene mucho sentido plantearse hasta qué punto las nuevas tecnologías pueden ayudarnos a mejorar la efectividad del citado principio, que debe gozar de reconocimiento formal en cualquier Estado que pretenda ser democrático. Al igual que las TICs están produciendo cambios sustanciales en las relaciones sociales y en el proceso de comunicación pública, estas también pueden ofrecer nuevas posibilidades en pro de la transparencia de los poderes estatales, la participación ciudadana –también en la toma de decisiones legislativas– y la reducción de los costes de acceso a la justicia. Para analizar el cambio de paradigma que la introducción de las nuevas tecnologías puede ocasionar en el Estado de Derecho, tendremos en cuenta fundamentalmente dos ítems: la transparencia y la responsabilidad de los poderes públicos; la participación de los ciudadanos en la *res publica* y en la elaboración de las leyes.

---

6 Me refiero al público liberal o burgués, que estaba integrado por burgueses, propietarios e intelectuales; en cualquier caso no representaba a toda la ciudadanía.

7 Las transformaciones del público son estudiadas en profundidad en Habermas, J. (1994). *Historia y crítica de la opinión pública*. México, D. F.: Gustavo Gili, p. 102.

8 Sirva como ejemplo Agrast, M., Botero, J. C. y Ponce, A. (2011). *WJP Rule of Law Index 2011.* Washington, D.C.: The World Justice Project. Para medir el grado en el que 66 países democráticos se adhieren al principio del imperio de la Ley y al Estado de Derecho, no en la teoría sino en la práctica, se han entrevistado a más de 66.000 personas y 2.000 expertos.

2. CAMBIO DE PARADIGMA EN LA EFECTIVIDAD DEL IMPERIO DE LA LEY

2.1. La transparencia electrónica

2.1.1. Noción de transparencia y estado de la cuestión en España

La transparencia de los poderes públicos ha sido definida como un «conjunto de institutos y de normas»[9] que caracteriza un modo de ser y actuar de los poderes públicos, en particular, y del sistema político, en general. La miscelánea de acepciones que admite la voz «transparencia» ha sido apuntada por diferentes autores[10], si bien nos gustaría subrayar determinados significados que se le atribuyen:

- Acceso público a documentos e información de los poderes públicos.
- Que la toma de decisiones del gobierno no se produzca a puerta cerrada.
- Publicidad de leyes, normas, decretos, directivas, etc.
- Publicidad de órdenes del día y de las actas de los órganos colegiados y de cualquier órgano decisorio.
- Publicidad de las resoluciones judiciales.
- Política de información activa, deber de la administración de ser proactiva en la gestión y difusión de la información relativa a su funcionamiento y actuación.
- Condiciones de las normas y actos de poderes públicos: presentación accesible, redacción simple, calidad de la legislación, coherencia, etc.

Con la lectura sistemática de los significados propuestos se observa que la transparencia se basa en el conocimiento público de la información del sector público tanto en su vertiente pasiva como activa, esto es, exige responder y proporcionar información cuando los ciudadanos la requieran pero también facilitar su acceso sin necesidad de que estos vayan detrás de la Administración pública, que debe ser proactiva en la gestión y difusión de la información relativa a su actuación.

Tal como sucede con el ideal del imperio de la Ley, la mayoría de las Constituciones de los Estados democráticos recogen también un principio general de publicidad de los poderes públicos o de transparencia. En España, no se recoge explícitamente en la CE un principio general de transparencia o publicidad de la actuación o inacción de los poderes estatales, sino que este se deriva de múltiples manifestaciones de la *lex legum*[11]. La transparencia, desde el

---

9 En estos términos se expresa Arena, G. (1993). Transparencia administrativa y democracia. *Revista Vasca de Administración Pública* (37), 9-20, p. 9.

10 Véase por todos Cotino, L. (2006). Transparencia y derecho de acceso a los documentos en la Constitución europea y en la realidad de su ejercicio. En Marc Carrillo y Hector López Bofill (coords.), *La Constitución Europea: actas del III Congreso Nacional de Constitucionalistas de España* (p. 285-308). València: Tirant Lo Blanch.

11 Sin ánimo de exhaustividad: la publicidad de las sesiones plenarias del Congreso y el Senado (art. 80 CE); el derecho de acceso ciudadano a los archivos y registros administrativos con la excepción de

punto de vista del ciudadano, es también un derecho, el de acceso a la información pública[12], que ha sido conceptualizado por la doctrina como un derecho constitucional autónomo, es decir, no se trata tan solo de una manifestación concreta de la libertad de recibir información –art. 20.1.d) CE–[13]. Tal interpretación encuentra su fundamento en el art. 105.b) de la Carta magna, que establece un principio de la actuación administrativa al exigir publicidad y transparencia de los archivos y registros administrativos. Más adelante, sin embargo, la Ley 30/1992, de régimen jurídico de las administraciones públicas (en adelante, LRJPAC) reconoció el derecho de acceso a la información pública[14] de una manera limitada, restringiéndolo[15] a base de excepciones que en cierta manera han constreñido sobremanera el texto constitucional[16].

---

aquello que afecte a la seguridad y defensa del Estado, la averiguación de delitos y la intimidad de las personas (art. 105 b) CE); la exigencia constitucional de la publicidad de las normas (art. 9.3 CE); el derecho a recibir información (art. 20.1.d) sobre asuntos de interés cívico; el derecho de toda persona a un proceso público (art. 24.2 CE) que exige la publicidad de las actuaciones judiciales, salvo las excepciones previstas en las leyes de procedimientos (art. 120.1 CE), y la obligación que las sentencias se pronuncien en la audiencia pública (art. 120.3 CE); por sensatez con las anteriores, la publicidad de las sentencias dictadas por el TC (art. 164.1 CE).

12 En perspectiva comparada, Suecia fue pionera con la aprobación de la Real Ordenanza sobre Libertad de Prensa, y se convirtió en el primer país del mundo que reconoció y reguló con una ley específica el derecho fundamental de acceso a la información pública, en el año 1766. La ley sueca proclamó expresamente el derecho de acceso de los ciudadanos suecos a la documentación oficial, con el objetivo de fomentar el libre intercambio de opiniones y la disponibilidad de la información completa. En concreto, el artículo 1 del capítulo segundo de la citada Ley sueca, titulado «Sobre el carácter público de los documentos oficiales», establece que «Every Swedish citizen shall be entitled to have free access to official documents, in order to encourage the free exchange of opinion and the availability of comprehensive information». Texto de la Ley de Libertad de Prensa Sueca recuperado con fecha de 23 de marzo de 2012, en http://bit.ly/d0EkJ8

13 Véase por todos Guichot, E. (2003). El nuevo derecho europeo de acceso a la información pública. *Revista de Administración Pública* (60), 283-316.

14 «Los ciudadanos, en sus relaciones con las Administraciones Públicas, tienen los siguientes derechos: […] H) Al acceso a los registros y archivos de las Administraciones Públicas en los términos previstos en la Constitución y en ésta u otras Leyes». Artículo 35.h) de la LRJPAC.

15 En la LRJPAC se establece que el acceso a la información sólo será permitido cuando los expedientes correspondan a procedimientos terminados en la fecha de la solicitud (art. 37.1); cuando no contengan datos referentes a la intimidad de las personas (art. 37.2); cuando terceros acrediten un interés legítimo y directo (art. 37.3); cuando no prevalezcan razones de interés público, por intereses de terceros más dignos de protección o cuando así lo disponga una Ley (art. 37.4); cuando no se trate de determinados registros y archivos (art. 37.5); en la forma que no se vea afectada la eficacia del funcionamiento de los servicios públicos debiéndose, a tal fin, formular petición individualizada de los documentos (art. 37.7).

16 Debe entenderse que con la actual regulación la excepción –el secreto de las actuaciones– corre el riesgo de convertirse en la regla general, cuando en realidad, el texto constitucional establece el secreto y la denegación como una anomalía, y en caso de excepción a la publicidad se exige que esta siempre sea proporcionada, justificada y motivada.

Vale la pena señalar que la regulación española prevista en la LRJPAC contrasta por completo con la tendencia internacional[17] de consagrar, reconocer y ampliar el derecho de acceso a la información; con el reconocimiento europeo del derecho de acceso a la información pública, que se ha producido de manera gradual desde el año 1997[18], pasando por la Carta de Derechos fundamentales de la Unión Europea[19] del año 2001 y por la Constitución Europea[20] del año 2005, hasta el Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos[21], del año 2009. De este modo, una asignatura pendiente en España sigue siendo la concreción y el desarrollo de garantías en pro de la transparencia[22], si bien todo indica que el legislador está próximo a despertar de su letargo como se desprende del anteproyecto de Ley de transparencia y acceso de los ciudadanos a la información pública[23].

17 A modo de ejemplo, la constitucionalización del derecho de acceso a la información pública se ha producido de manera progresiva a nivel internacional en las últimas décadas: en la República de Sudáfrica y en Rusia (1993), en Brasil (1997), en Ecuador (1998 y 2004), en Venezuela (1999), en Francia (2000), en Paraguay (2001), en Perú (2002), en México y Argentina (2003), en la República Dominicana, en Serbia y en la India (2004), por citar algunos países. Para observar un análisis detallado de la tendencia universal de constitucionalizar y reforzar el derecho de acceso a la información pública vid. Bernardí, X. (2006). *Administracions públiques i Internet. Elements de dret públic electrònic.* Barcelona: Fundació Carles Pi i Sunyer, Estudis 21, p. 179-183.

18 «Todo ciudadano de la Unión, así como toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, tendrá derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión, con arreglo a los principios y las condiciones que se establecerán de conformidad con los apartados 2 y 3». Artículo 255.1 del Tratado de la Comunidad Europea, introducido por el tratado de Ámsterdam de 1997.

19 «Todo ciudadano de la Unión o toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión». Artículo 42 de la Carta de Derechos fundamentales de la Unión Europea.

20 «Todo ciudadano de la Unión y toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene derecho a acceder a los documentos de las instituciones, órganos y organismos de la Unión, cualquiera que sea su soporte». Artículo 102 del Tratado por el que se establece una Constitución para Europa.

21 «Artículo 2 - Derecho del acceso a los documentos públicos 1) Cada Parte garantizará el derecho de cualquiera, sin discriminación de ningún tipo a acceder, bajo petición, a los documentos públicos en posesión de las autoridades públicas. 2) Cada Parte tomará las medidas necesarias en su ordenamiento jurídico para hacer cumplir las previsiones sobre acceso a documentos públicos previstas en este Convenio». Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos recuperado con fecha de 23 de marzo de 2012, en http://www.derecom.com/numeros/pdf/convenio.pdf

22 La pereza y falta de compromiso que se detecta por parte de los poderes públicos en la regulación de la transparencia electrónica ha sido subrayada por diferentes autores. Véase por todos Cotino, L. (2007). El débil compromiso normativo por la transparencia y participación electrónicas. Situación actual y posibilidades de futuro. En Lorenzo Cotino Hueso (Coord.), *Democracia, participación y voto a través de las nuevas tecnologías* (p. 35-86). Granada: Comares, Colección Sociedad de la Información núm. 13.

23 Texto recuperado con fecha de 24 de marzo de 2012, en http://bit.ly/9Owhn6

2.1.2. Publicidad, transparencia y sometimiento de los poderes a la Ley en el Estado de Derecho

Dejando ya de lado el caso español, lo cierto es que es comúnmente aceptado que la transparencia y el principio de publicidad de los poderes públicos están intrínsecamente conectados con el Estado de Derecho, puesto que los primeros promueven la rendición de cuentas y facilitan la formación de una opinión pública libre que controla las acciones que llevan a cabo los poderes legislativo, ejecutivo y judicial. La transparencia permite controlar la actuación del gobierno y la administración, y a su vez facilita participar e interactuar con los mismos en un sistema de gobernanza. Así, por ejemplo, no es de extrañar que en el marco de la Unión Europea, el Tratado de Lisboa señale la transparencia como uno más de los principios del buen gobierno vinculado al principio democrático y a las posibilidades reales de participación de los ciudadanos[24]. De un lado, la superioridad o primacía de la Ley solo es verosímil si esta y su proceso de elaboración son transparentes, accesibles y representan la voluntad general, esto es, la voz «Ley» se concibe en el pensamiento liberal como la autodeterminación de la sociedad sobre sí misma, sin imposiciones ajenas, y esto exige participación ciudadana y confianza informada en el legislador, que también está sometido a la leyes en general y esencialmente a la Constitución como norma suprema. En ese marco teórico aparece también el principio de publicidad del proceso judicial, ya que, como excelentemente apunta Ernesto Pedraz Penalva, «con la presencia en las actuaciones judiciales de elementos no intervinientes en ellas se refuerza el control de la generalidad de la ley y de su eficacia (y general) aplicación»[25]. Por otro lado, debe tenerse en cuenta que la accesibilidad de la información relativa a la actuación de los diferentes poderes estatales ayuda a enriquecer el debate público y permite a los ciudadanos ejercer un control democrático sobre los mismos[26]. En otros términos, si se aboga por la transparencia se robustece el principio democrático, toda vez que se abren y ensanchan los cauces de comunicación entre los ciudadanos y quienes se ocupan de la gestión de los asuntos públicos.

En cualquier caso, y una vez observadas, aunque sucintamente, las razones que vinculan el principio de publicidad de los poderes con el Estado de Derecho y la supremacía de la Ley, puede afirmarse sin temor a caer en error que el nivel de transparencia de los poderes es una buena muestra de la calidad democrática. La configuración legal del derecho de acceso a la información pública y su reconocimiento formal contribuye directamente a mejorar la calidad de la democracia[27]. De hecho, los niveles de apertura y accesibilidad de la

24 «1. A fin de fomentar una buena gobernanza y de garantizar la participación de la sociedad civil, las instituciones, órganos y organismos de la Unión actuarán con el mayor respeto posible al principio de apertura». Art. 16 A del Tratado de Lisboa.

25 Pedraz, E. (1986). Notas sobre publicidad y proceso. En VV.AA., *El Poder Judicial en el conjunto de los Poderes del Estado y de la Sociedad* (p. 128). Madrid: Consejo General del Poder Judicial.

26 El principio de control democrático de los poderes nace ligado también a la elaboración teórica del ideal del imperio de la Ley.

27 Luego no es de extrañar que en el Anteproyecto de Ley de transparencia y acceso de los ciudadanos a la información pública se afirme que «la transparencia en la actividad pública no debe verse como

información pública son aceptados universalmente como uno de los principales indicadores de calidad de los sistemas democráticos. A todo ello se refería Louis Brandeis, quien en su día fue juez del Tribunal Supremo de los Estados Unidos, al defender que «publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman»[28]. Unas palabras escritas en clara referencia al papel crucial que juegan la transparencia y la responsabilidad de los poderes en una sociedad democrática, así como a la importancia de poner la información a disposición del público. Incluso algunos autores han llegado a elevar la publicidad de los poderes públicos a categoría moral, apuntando que son injustas todas las acciones relativas al derecho de los demás hombres cuya máxima no sea susceptible de publicidad[29]. En un terreno más práctico, parece evidente que un gobierno transparente es propenso a prestar un mejor servicio a la sociedad, y en caso contrario, la transparencia actúa como salvaguarda de la ciudadanía frente a la mala administración, puesto que esta puede conocer y criticar con fundamento su actividad, así como vigilar atentamente la prestación de servicios, el ejercicio de las potestades y el destino de los recursos públicos.

2.1.3. El empleo de las TICs a propósito de la transparencia

Vista la importancia que la transparencia de los poderes alcanza en una sociedad democrática parece lógico trabajar en la premisa que entiende que las TICs pueden simplificar y facilitar la accesibilidad a la información relativa a los poderes estatales y dar un nuevo sentido al derecho de acceso a la información pública. De hecho, ya hace tiempo que se repite en el debate público la idea de incorporar las nuevas tecnologías en la actividad del

---

la respuesta forzada por la eventual demanda de información por parte de los ciudadanos, sino como un principio rector de la actividad pública; como el modo característico de actuación de los poderes públicos en una democracia constitucional, en la que los poderes actúan sometidos a la Constitución y al resto del ordenamiento, con criterios que atienden al interés general, y responden de su gestión ante los ciudadanos». Texto recuperado con fecha de 24 de marzo de 2012, en http://bit.ly/9Owhn6

28 Brandeis, L. (1913). What Publicity Can Do. *Harper's Weekly*, recuperado con fecha de 24 de marzo de 2012, en http://goo.gl/dEbaI

29 «No hay que considerar este principio como un mero principio *ético* (perteneciente a la doctrina de la virtud) sino que hay que considerarlo también como un principio *jurídico* (que afecta al derecho de los hombres). Un principio que no pueda manifestarse *en alta voz* sin que se arruine al mismo tiempo mi propio propósito, un principio que, por lo tanto, debería permanecer *secreto* para poder prosperar y al que no puedo *confesar públicamente* sin provocar indefectiblemente la oposición de todos, un principio semejante sólo puede obtener esta universal y necesaria reacción de todos contra mí, cognoscible *a priori*, por la injusticia con que amenaza a todos. – Es, además, un principio *negativo*, es decir, sólo sirve para conocer lo que *no es justo* con respecto a los otros». Kant, I. (1998). *Sobre la paz perpetua* (p. 61-62). Madrid: Tecnos. Citado en Cotino, L. (2011). Del «deber de publicidad» de Brandeis al «Open Government» de Obama (p. 2). Regulación y control de la información pública a través de las nuevas tecnologías. Ponencia invitada en el Congreso Internacional «La protección de los Derechos Humanos para las Defensorías del Pueblo», 1-3 de junio, AECI – Universidad Alcalá de Henares, recuperado con fecha de 14 de julio de 2011, en http://www.goo.gl/br3rs

poder ejecutivo y legislativo a propósito de dar mayor significado y alcance al principio de publicidad. A principios de los años noventa se vinculó la transparencia con las TICs por vez primera. Para ser más exactos, fue en el año 1993 cuando el pionero *Informe Gore*[30] introdujo un principio[31] que planteaba la importancia de emplear las nuevas tecnologías para mejorar el flujo informativo entre las Administraciones Públicas y la ciudadanía, con el fin de dotar de mayor efectividad al derecho del público a informarse y fortalecer, por ende, la configuración libre de la opinión pública.

Desde la aparición del *Informe Gore* hasta la actualidad, muchas han sido las oportunidades tecnológicas de abrir, por lo que respeta a la trasparencia, el gobierno a la ciudadanía. En este período temporal de casi dos décadas han surgido conectados a la *e-transparency* los conceptos de gobierno electrónico –*e-government*– y democracia electrónica –*e-democracy*–. Sirva como ejemplo el precursor informe del G-8 del año 2001 sobre democracia electrónica en el que se observaba la necesidad de «asegurar el acceso y la accesibilidad de la información del gobierno nacional. Una e-democracia debe permitir la consulta pública en línea, y solo puede ser establecida en dos pilares: la consulta electrónica y la accesibilidad»[32]. Y dentro de ese interesante objetivo se formulaban los siguientes principios que deberían regir el acceso a la información pública:

«1 Recognoscibilidad y localizabilidad: el público deben conocer qué información esta accesible, y cómo y dónde puede ser localizada.

2 Disponibilidad: la información debe estar dispuesta en formato digital y ser accesible en medios y soportes electrónicos.

3 Manejabilidad: los ciudadanos deben poder manejar la cantidad y complejidad de la información, así como se capaces por sí mismos de encontrar la información incluso si es necesario por medio de sistemas de búsqueda dispuestos por los gobiernos.

4 Precio razonable: el precio no debe crear barreras.

5 Responsabilidad y confianza: los usuarios deben poder confiar en la corrección, sistematización y autenticidad de la información.

30 Este informe fue promovido por Al Gore cuando este era Vicepresidente de los Estados Unidos de América. En concreto, el informe fue sido traducido por Fernández, R. (1994). La Infraestructura Nacional de Datos (NII) de Estados Unidos de América: Agenda para la Acción. *Novática* (110), recuperado con fecha de 14 de julio de 2011, en http://www.ati.es/novatica/1994/jul-ago/gore110.html

31 Más concretamente, se trata del noveno principio del *Informe Gore*: «La Administración tratará de asegurar que los organismos federales, de acuerdo con las Administraciones Locales y de los Estados de la Unión, utilicen la NII [*se refiere a la Infraestructura Nacional de Datos*] para incrementar la información disponible al público, asegurando que el inmenso caudal de información en poder de las Administraciones Públicas está disponible para los ciudadanos de modo fácil y equitativo».

32 VV. AA. (2001). *Online consultation in GOL countries. Initiatives to foster e-democracy*, Government Online International Network, recuperado con fecha de 23 de marzo de 2012, en http://bit.ly/iRleb5

6 Claridad: la información ha de ser todo lo clara posible en términos de contenido, contexto y presentación.

7 La información debe ser preferiblemente accesible para las personas limitadas física o psíquicamente»[33].

A nuestro juicio, las TICs pueden ser especialmente útiles para garantizar la eficacia de la gran mayoría de principios citados que se indicaron en el informe del G-8, al permitir el escrutinio de miles de datos que obran en manos de las Administraciones públicas, convenientemente relacionados y cruzados, y ayudar a detectar rápidamente procesos dudosos o decisiones no justificadas. La tecnología faculta la simplificación del tratamiento de la información, mejora la manejabilidad y el acceso a esta mediante los sistemas de consulta, permite la plena disponibilidad durante las 24 horas del día de los documentos y archivos liberados, posibilita la gratuidad en el acceso, aumenta la recognoscibilidad y localizabilidad de la información, fomenta la responsabilidad y confianza, facilita la reutilización de la información del sector público[34], etc. Lo anterior quiere decir entonces que las nuevas tecnologías son susceptibles de dar una mayor extensión a la transparencia en términos de calidad, garantizando la igualdad en el acceso y facilitando la accesibilidad de la información. Más concretamente, se perciben ventajas en un doble sentido. De un lado, encontramos los beneficios técnicos en el proceso de difusión de la información; de hecho, sin las TICs sería imposible la plena accesibilidad a la información –disponibilidad 24 horas al día, reducción de costes económicos y temporales para encontrar lo que se busca, etc.– y el aumento de la calidad en el tratamiento y usabilidad de la misma. La transparencia electrónica permite entonces la accesibilidad permanente a la información relacionada con la actividad de los poderes estatales sin necesidad de una petición concreta de los ciudadanos, es decir, se trata de un acceso activo a la información «que se garantiza a través de la difusión generalizada de la información mediante la creación de sistemas de difusión de la información por parte de los poderes públicos»[35]. Por otro lado, también encontramos beneficios relacionados con la gobernabilidad, y es que al automatizar los procesos para dar publicidad a la información, se elimina la posibilidad de que el ser humano –corruptible– intervenga en los mismos. La

33 Ibídem, p. 9.

34 La reutilización es definida como «el uso de documentos que obran en poder de las Administraciones y organismos del sector público, por personas físicas o jurídicas, con fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública». Artículo 3 de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. De eso modo, la difusión de información del sector público no se produce tan solo por la acción de las Administraciones públicas, sino también por la eventual actuación de los ciudadanos que difunden y amplifican la información que consideran oportuna a través de la web 2.0. Sobre este particular véase Cerrillo, A. (2011). Web 2.0 y la participación ciudadana en la transparencia administrativa en la sociedad de la información. En Lorenzo Cotino Hueso (ed.), *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías* (p. 131-148). València: Servei de Publicacions de la Universitat de València.

35 Cerrillo, A. (2005). E-información: hacia una nueva regulación del acceso a la información. *Revista de Internet, Derecho y Política* (1), 1-16, p. 13.

tecnología facilita la divulgación de la información y amplia su difusión sin necesidad de intervención humana, lo que a ojos del público debería generar una mayor confianza en la información que se obtiene.

Por todo ello sorprende que la transparencia electrónica se haya puesto, una vez tras otra, en la cola de las prioridades gubernamentales[36]. No obstante, a día de hoy, la transparencia y la publicidad de los poderes mediante las nuevas tecnologías parece gozar de un consenso generalizado y de un compromiso gubernamental nunca antes observado, quizás por la nueva moda introducida por el presidente Obama: «My Administration is committed to creating an unprecedented level of openness in Government. We will work together to ensure the public trust and establish a system of transparency, public participation, and collaboration. Openness will strengthen our democracy and promote efficiency and effectiveness in Government»[37]. Se trata de un verdadero cambio de paradigma, que bajo la voz «*Open Government*» pretende emplear decididamente las TICs en las relaciones entre la ciudadanía y la Administración pública, creando una nueva relación entre ambos más cercana, sin tantos costes –temporales y económicos– y con nuevas opciones de participación y colaboración. Esto difiere por completo de la postura simplista que solo enlaza las TICs, en general, y las herramientas 2.0, en particular, para aplicarlas en los procedimientos administrativos ya existentes. La transparencia constituye uno de los pilares de la noción «gobierno abierto», que exige apertura del gobierno para cimentar la confianza ciudadana y conseguir una gestión más eficiente y eficaz de los asuntos públicos. En este contexto se ha empezado a hablar también del *Open Data* –datos abiertos-, que se integraría dentro del propósito de dotar de mayor transparencia al gobierno, poniendo a disposición de los ciudadanos información que obra en su poder para que los ciudadanos la reutilicen con el fin de analizar y evaluar la gestión pública, o creen servicios derivados de la misma. El *Open Data* aumenta la interoperabilidad entre administraciones, facilitando la creación de servicios para que la ciudadanía reutilice datos de diferentes administraciones, y promueve la eficiencia en la ordenación interna y la clasificación de los datos que obran en poder de la administración[38].

2.2. Participación ciudadana en la toma de decisiones legislativas

La participación de la ciudadanía en la *res publica* es, sin lugar a dudas, otro de los ítems que puede ayudarnos a calibrar la eficacia del imperio de la Ley y la vigencia del Estado de

36 En una línea muy similar, Lorenzo Cotino recuerda que «esta proclamación de la transparencia electrónica no es algo esencialmente nuevo puesto que figuraba como elemento esencial desde 1993. Hoy día de hecho sigue enfocándose hacia la reutilización de la información, la información pública como materia prima. Algo hoy día rebautizado como «Open Data» y con una finalidad esencialmente económica». Cotino, L. (2011). Del «deber de publicidad» de Brandeis… *op. cit*, p. 15.

37 Obama, B. (2010). Memorandum for the Heads of Executive Departments and Agencies. Subject: Transparency and Open Government. Recuperado el 28 de marzo de 2011, en http://1.usa.gov/8eo8tl

38 Sirvan como ejemplo los portales web http://data.gov.uk/data y http://dadesobertes.gencat.cat

Derecho en la práctica. Este principio está conectado, como hemos apuntado *supra*, con la noción de transparencia y a su vez con el principio democrático. Luego no es de extrañar que la participación de la ciudadanía sea otro de los pilares del nuevo paradigma «Open Government». Debe entenderse que a mayor participación y compromiso ciudadano con lo público, mayor es la eficacia del gobierno, que mejora la calidad de sus decisiones fruto de la apertura y el contacto directo con las opiniones y problemas de los ciudadanos. En este ámbito, muchas son las posibilidades que las nuevas tecnologías nos ofrecen y que viajan desde la configuración de un nuevo sistema que tenga en cuenta la opinión de los ciudadanos en la toma de decisiones hasta el voto electrónico[39].

Las constituciones democráticas suelen incluir algún tipo de participación del público, más allá de la votación formal. Por ejemplo, la CE recoge en diferentes preceptos una serie de derechos relativos a la participación ciudadana en la configuración de la esfera pública, como muestra de la importancia de la pluralidad política e ideológica de la ciudadanía en una sociedad democrática: derechos de reunión, asociación y participación reconocidos en los artículos 21.1, 22.1 y 28.1 CE. Se trata de derechos de titularidad individual vinculados al Estado social y democrático, que ayudan a confeccionar una esfera que faculta a los ciudadanos a unirse para actuar y expresarse de acuerdo con sus convicciones, ideas y opiniones. Las nuevas tecnologías pueden abrir nuevas vías para el ejercicio de esos derechos, simplificando los procesos y promoviendo la cooperación e intervención de la ciudadanía en la confección de la cosa pública. Entiéndase que esta es una perspectiva mucho más ambiciosa que la lectura limitada que sólo enlaza participación democrática y TICs con referencia al voto electrónico[40]. Sin ir más lejos, la web 2.0 y las redes sociales facilitan la creación de foros globales o espacios webs de reunión, debate y discusión entre ciudadanos. Las aplicaciones tecnológicas pueden abrir una magnífica oportunidad para hacer parcialmente efectivo el ideal de democracia deliberativa como sistema político donde la toma de decisiones se realiza después de la discusión entre ciudadanos libres e iguales[41]. En forma sintética, los derechos de reunión, asociación y participación pueden llegar a tener un alcance antaño inimaginable gracias al empleo de las TICs por parte de los poderes públicos. El dialogo ciudadano sin jerarquía sobre los temas de interés cívico y la adopción de decisiones encaja sin problemas o debería hacerlo en cualquier sistema político democrático. En la Red de redes es posible la aportación de ideas, opiniones y juicios que ayuden a enriquecer la toma de decisiones que afectan, precisamente, a aquellos que han participado en la formación de la misma. Y todo

39 En este mismo sentido, véase Simón Castellano, P. (2011). Los límites jurídico-constitucionales de la Administración electrónica en España y el Open government. Revista *Aranzadi de Derecho y Nuevas Tecnologías* (27), 67-85.

40 Esta postura simplista que entronca TIC y participación ciudadana tan solo por el voto electrónico ya ha sido excelentemente refutada por Cotino, L. (2005). El voto electrónico o la casa por el tejado: La necesidad de construir la democracia y la participación electrónicas por los cimientos. En Lorenzo Cotino Hueso (Coord.), *Libertades, democracia y gobierno electrónicos* (p. 328-347). Granada: Comares, Colección Sociedad de la Información núm. 9.

41 Véase Elster, J. (2001). *La democracia deliberativa*. Barcelona: Gedisa.

ello, evidentemente, con límites, ya que la efectividad absoluta del ideal de democracia deliberativa es inimaginable y el empleo de las TICs a propósito de la participación ciudadana no es la panacea de todos los males, entre otras cosas, porque no es tarea fácil determinar si «el sistema democrático requiere o no mayores y más extensas dosis de participación popular, y saber qué mecanismos pueden contribuir a ello sin cargar en exceso (de costes de tiempo y de transacción) los ya fatigados hombros de la ciudadanía»[42].

En cualquier caso, las TIC, Internet y la web 2.0 son «nuevas» realidades sociales que pueden facilitar enormemente la participación ciudadana; precisamente por ello, tienen que ser consideradas y recibidas por el Derecho Constitucional. Cabe recordar que más allá del papel normativo de la Constitución, esta también cumple con una función transformadora *ad hoc* de la consolidación del sistema democrático[43]. En este sentido, las características de Internet que, a través de la interactividad multidireccional posibilitan la articulación e institucionalización de procesos de participación cívica en la cosa pública, tienen que ser obligatoriamente observadas en la configuración constitucional cara al futuro. De hecho, el marco constitucional no solo prevé la participación ciudadana en los asuntos públicos a nivel formal, tal como establece el art. 23.1 CE –de manera directa o a través de los representantes escogidos en las elecciones periódicas por sufragio universal–, sino que también incorpora, en el art. 9.2 CE, un mandato a los poderes públicos para que promuevan y faciliten la participación de todos los ciudadanos en la vida política, económica, cultural y social.

Un buen ejemplo de cómo emplear las TICs para simplificar los procesos de participación ciudadana en la elaboración de las leyes es el reglamento de la llamada Iniciativa Ciudadana Europea (en adelante, ICE). Para situarnos, el Tratado de Lisboa incorpora una novedad en el art. 11.4 respecto a las previsiones de participación ciudadana previstas en anteriores Tratados de la Unión Europea, con la salvedad del *non nato* Tratado por el que se establece una Constitución por Europa. Se trata de la inclusión de la ICE como una herramienta para canalizar la voluntad de participación ciudadana en el proceso legislativo; que se concreta en los siguientes términos: «un grupo de al menos un millón de ciudadanos de la Unión, que sean nacionales de un número significativo de Estados miembros, podrá tomar la iniciativa de invitar a la Comisión Europea, en el marco de sus atribuciones, a que presente una propuesta adecuada sobre cuestiones que estos ciudadanos estimen que requieren un acto jurídico de la Unión en aplicación de los Tratados». Esta herramienta de democracia participativa, que no se concreta ni formula como un derecho subjetivo, tiene un ámbito objetivo que incluye todas las materias respecto de las cuales la Comisión Europea tiene atribuida iniciativa o competencia legislativa. La ICE ha recibido una valoración positiva por

42 Subirats, J. (2002). Los dilemas de una relación inevitable: innovación democrática y tecnologías de la información y de la comunicación. En Heriberto Cairo (comp.), *Democracia digital: límites y oportunidades* (p. 89-113, la cita se encuentra en la p. 96). Madrid: Trotta.

43 En este sentido vid. por todos Álvarez Conde, E. (2003). *Curso de derecho constitucional: El Estado constitucional. El sistema de fuentes. Los derechos y libertades*. Madrid: Tecnos, p. 152.

parte de la doctrina[44], que destaca la posibilidad de que los ciudadanos ocupen «an active role in opening deliberations about a particular legislative request»[45].

Con todo, y para lo que aquí interesa, el reciente Reglamento (EU) núm. 211/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, sobre la ICE (en adelante, Reglamento ICE), ha incorporado las TICs como elemento estructural para garantizar la participación ciudadana, por ejemplo, al permitir la recogida de apoyos vía Internet. Más concretamente, el Reglamento ICE establece que los apoyos podrán recogerse en papel o electrónicamente –art. 5.2– y señala que a más tardar el 1 de enero de 2012[46] la Comisión aprobará las especificaciones técnicas –art. 6.5– y establecerá y mantendrá programas de código abierto y gratuitos[47] que incorporen las características técnicas y de seguridad necesarias –art. 6.2–. De ese modo, lo realmente novedoso es que la ICE se ha concebido teniendo en cuenta los principales riesgos y posibilidades que ofrecen las TICs[48], al establecerse un procedimiento que está basado en la suma de apoyos a través de nuevas tecnologías e Internet a la par que se incorporan las características técnicas que garantizan la seguridad y la protección de los datos personales. Obviamente, habrá que esperar y comprobar cual es el impacto real que tiene la ICE, pero paga la pena señalar ya en este momento que tal herramienta constituye un buen ejemplo de cómo el uso de las nuevas tecnologías puede facilitar la participación directa de la ciudadanía en el procedimiento legislativo.

---

44 «Al atribuir a los ciudadanos las mismas facultades de promover esa iniciativa [*legislativa*] de las que ya disfrutan el Consejo de Ministros y el Parlamento Europeo se subsana una evidente carencia. Ya es hora de que se ofrezca a los ciudadanos la oportunidad de intervenir por sí mismos, sin la mediación de los partidos, en el proceso de construcción de la Europa del siglo XXI, en el futuro gobierno de Europa, más allá de su participación periódica en las elecciones. Estamos ante la primera herramienta transnacional de democracia participativa, una fórmula pionera en el mundo (es la primera vez que una organización supranacional adopta un instrumento de participación directa), que tal y como va a regularse no presenta contraindicaciones». Bilbao Ubillos, J. M. (2011). La iniciativa ciudadana europea (art. 11.4 TUE). En Emilio Pajares Montolío (coord.), *Participación ciudadana y procedimiento legislativo: de la experiencia española a la iniciativa ciudadana europea* (p. 47-100, la cita se encuentra en la p. 98). Madrid: Centro de Estudios Políticos y Constitucionales.

45 Cuesta López, V. (2010). The Lisbon Treaty's Provisions on Democratic Principles: A Legal Framework for Participatory Democracy. *European Public Law* 16 (1), 123–138, p. 136.

46 La Comisión Europea ya ha adoptado las especificaciones técnicas para sistemas de recogida a través de páginas web, mediante el Reglamento de Ejecución (UE) núm. 1179/2011 de la Comisión, de 17 de noviembre de 2011, por el que se establecen las especificaciones técnicas para sistemas de recogida a través de páginas web, de conformidad con el Reglamento ICE. El documento puede consultarse en Internet, en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:301:0003:0009:EN:PDF

47 Ya está disponible el software para la recogida de firmas online elaborado por la Comisión Europea. Recuperado el 23 de marzo de 2012, en https://joinup.ec.europa.eu/software/ocs/release/100

48 Véase por todos Cotino Hueso, L. (2011). El Reglamento de la Iniciativa Ciudadana Europea de 2011: Su especial regulación de la recogida de apoyos vía internet y de la protección de datos de los ciudadanos. *Revista de Derecho Político* (81), 323-378.

3. LA CONSTITUCIÓN 2.0 Y EL PROCESO CONSTITUYENTE ISLANDÉS

Un buen ejemplo de las transformaciones que el empleo de las TICs puede implicar para las nociones Constitución, Imperio de la Ley y Estado de Derecho, es el que proviene del «laboratorio» islandés. La crisis económica y política obligó a Islandia a refundarse; lo sorprendente ha sido la manera como se ha gestionado el proceso constituyente, que ha destacado precisamente por su transparencia y por las facilidades de participación y debate. La tecnología colaborativa 2.0 se ha explotado para abrir la discusión a toda la ciudadanía sin un protagonismo exclusivo ni decisivo de las fuerzas políticas, más debilitadas que nunca. Es cierto que normalmente las asambleas constituyentes están abiertas a algún tipo de escrutinio público, por ejemplo, con el referéndum final que precede la aprobación de la Constitución –si bien el texto ha sido previamente escrito por unos pocos privilegiados–. A pesar de que el referéndum tradicionalmente ha servido para legitimar el proceso constitucional, tal herramienta se presenta como insuficiente en un momento en el que se observa una profunda brecha entre las instituciones, la política formal, los representantes políticos y la sociedad[49]. En el caso de la redacción de la Constitución para Islandia esa brecha se selló, entre otras cuestiones, porque el texto constitucional fue el resultado de un debate público, inclusivo y cooperativo producido en el universo 2.0. De hecho, la nueva Constitución de Islandia ha sido la primera en nacer completamente bajo la mirada atenta de un público global. Veamos algunos ejemplos de todo esto: los miembros del Consejo Constitucional islandés interactuaron regularmente con los ciudadanos que libremente se implicaron a través del portal web habilitado a tal efecto; cada semana los proyectos relativos al texto de la nueva Constitución fueron compartidos a través de un sitio Web público; mediante un boletín electrónico se informaba regularmente de los últimos acontecimientos relacionados con proyecto constitucional; cada semana se retransmitían en directo las reuniones del Consejo Constitucional en la página web y en otras redes sociales como *Facebook* y *Youtube*. Asimismo, las Reglas de Procedimiento del Consejo Constitucional[50] (en adelante, RPCC) prescribían la transparencia y participación electrónica de la ciudadanía a lo largo del proceso. Por lo que a transparencia se refiere, las reuniones del Consejo Constitucional fueron grabadas y compartidas en la página web en el plazo máximo de un día desde su celebración –art. 9 RPCC–, facilitando tanto las grabaciones como las transcripciones de las discusiones –art. 11 RPCC–. En lo relativo a la participación, la web del Consejo Constitucional incluyó un apartado dedicado a las propuestas e iniciativas de los ciudadanos –art. 14 RPCC–, posibilitando participar directamente en la elaboración de la *lex superior*. No es cuestión para nada baladí, puesto que todas las enmiendas propuestas al texto fueron discutidas y debatidas antes de que el Consejo Constitucional islandés las votara –art. 15 RPCC–. Las votaciones, que se realizaron artículo por artículo, también fueron retransmitidas. En defini-

49 Véase por ejemplo Taibo, C. (2011). *Nada será como antes: Sobre el movimiento 15-M*. Madrid: Catarata.

50 Constitutional Council of Iceland. (2011). *Rules of procedure*. Recuperado con fecha de 23 de marzo de 2012, en http://stjornlagarad.is/english/rules-of-procedure/

tiva, se trata de un escenario completamente diferente, en el que la opinión de la ciudadanía es escuchada en todo momento en el marco de un proceso transparente de elaboración legislativa y, especialmente, de confección de la norma suprema a la que todos se someten. Nunca aquello de que «la Constitución emana del pueblo soberano» fue tan cierto como en el caso de la Constitución 2.0. Un proceso transparente y participativo permite alcanzar un consenso social con mayor compromiso cívico y con una legitimidad incuestionable. Y esta última, a su vez, favorece la responsabilidad cívica y política en la construcción del futuro común del país. Islandia ha sabido usar las TICs como nunca antes para abrir su proceso constitucional al mundo entero y atraer la atención de su empoderada ciudadanía, con lo que ha fortalecido decisivamente su sistema político e instituciones.

Ahora bien, ¿es el modelo de proceso constituyente 2.0 islandés exportable a otros países? Se plantean dudas en diferentes sentidos. En primer lugar, todas las relacionadas con las dificultades prácticas para tener en cuenta las aportaciones cívicas al texto constitucional en un país considerable en número de habitantes. Lógicamente, un proceso participativo es más económico en un pequeño país como Islandia, donde la población no excede de los 400.000 habitantes. La deliberación y el debate de las diferentes aportaciones ciudadanas generan costes, muchos de ellos provenientes también de las medidas de seguridad y la protección de datos personales. En segundo lugar se proyectan algunos interrogantes sobre si la ciudadanía está preparada para tanta dosis de democracia directa. O dicho con otras palabras, dar la oportunidad de participar en los procesos de formulación de políticas y elaboración legislativa no garantiza que los ciudadanos participen. A nuestro juicio, este no es realmente un problema, ya que no se trata solo de participar, sino de posibilitar la participación cívica en la elaboración de las leyes. Con el mero hecho de dar la opción se legítima el proceso y se fomenta la confianza pública en la Constitución que resulta del mismo.

4. CONCLUSIONES

A lo largo de este trabajo hemos estudiado como los principios de publicidad y transparencia de los poderes estatales y de participación ciudadana, que están conectados con las nociones de imperio de la Ley, Estado de Derecho y Constitución, pueden tener un nuevo significado mediante el empleo de las nuevas tecnologías. Más concretamente, la idea de que nadie está por encima de las leyes y la Constitución, que emana del pueblo que es soberano, obtiene un nuevo alcance y significación. Tradicionalmente, la legitimación de la Constitución ha resultado de un ejercicio final de democracia directa, esto es, el referéndum popular sobre el texto constitucional propuesto por unos cuantos elegidos. Y el resto de las leyes tiene sus cimientos, por lo que a legitimidad se refiere, en un sistema constitucional representativo. Entre otras cosas, porque durante mucho tiempo se ha entendido que un Estado no puede ser gobernado por muchos[51]. Sin embargo, tal como muestra el caso islan-

51 Decía Rousseau: «Tomando el término en su rigurosa acepción, no ha existido nunca verdadera democracia, ni existirá jamás. Va contra el orden natural que el gran número gobierne y el pequeño

dés, las nuevas tecnologías facilitan la apertura de los procesos legislativos ante un público global, permiten la plena accesibilidad a los debates y textos relacionados con el proyecto constitucional y fomentan la participación cívica en la elaboración de la Carta magna. La ciudadanía puede ejercer un rol activo en la toma de decisiones legislativas mediante la tecnología colaborativa, lo que incluye no solo las posibilidades de voto electrónico, sino también las ingentes oportunidades de acceder a la información del proceso constituyente y de participar con comentarios, ideas y sugerencias que tras el debate y votación del Consejo Constitucional en cuestión pueden ser incorporadas al texto constitucional. Todo ello debe ser valorado positivamente, puesto que la participación en la redacción del texto constitucional implica un mayor compromiso cívico con este, y comporta la responsabilidad ciudadana con la construcción del futuro del país; mientras que la transparencia electrónica reporta una legitimidad moral incuestionable tanto para el proceso como para el texto resultante. Se trata de la Constitución 2.0 y del Estado de e-Derecho, una realidad que puede ayudar a reforzar la legitimidad democrática de los sistemas políticos y de las instituciones que, si bien a día de hoy nos representan con plena legitimidad y autoridad, están en sus cotas más bajas de valoración, credibilidad y confianza, tal como muestran los multitudinarios movimientos de protesta e indignación como el 15-M. O dicho con otras palabras, a pesar de que la democracia se presenta como el más legítimo de los regímenes políticos, la mayoría de elementos con los que se identifica se encuentra en crisis, quizás porque esta se ha reducido a una simple técnica de recambio periódico de las élites gobernantes. En ese estado de cosas las TICs son idóneas para acabar con tal paradoja y contribuir enormemente a reducir la distancia entre el ideal democrático y su práctica efectiva.

5. BIBLIOGRAFÍA

Agrast, M., Botero, J. C. y Ponce, A. (2011). *WJP Rule of Law Index 2011.* Washington, D.C.: The World Justice Project.

Arena, G. (1993). Transparencia administrativa y democracia. *Revista Vasca de Administración Pública* (37), 9-20.

Bernardí, X. (2006). *Administracions públiques i Internet. Elements de dret públic electrònic.* Barcelona: Fundació Carles Pi i Sunyer, Estudis 21.

Bilbao Ubillos, J. M. (2011). La iniciativa ciudadana europea (art. 11.4 TUE). En Emilio Pajares Montolío (coord.), *Participación ciudadana y procedimiento legislativo: de la experiencia española a la iniciativa ciudadana europea* (p. 47-100). Madrid: Centro de Estudios Políticos y Constitucionales.

sea gobernado. No se puede imaginar que el pueblo permanezca continuamente reunido en asamblea para vacar a los asuntos públicos, y fácilmente se ve que no podría establecer para esto delegaciones sin que cambie la forma de administración». Rousseau, J. J. (1978). *El contrato social*. Madrid: Aguilar, p. 70.

Brandeis, L. (1913). What Publicity Can Do. *Harper's Weekly*, recuperado con fecha de 24 de marzo de 2012, en http://goo.gl/dEbaI

Cerrillo, A. (2005). E-información: hacia una nueva regulación del acceso a la información. *Revista de Internet, Derecho y Política* (1), 1-16.

Cerrillo, A. (2011). Web 2.0 y la participación ciudadana en la transparencia administrativa en la sociedad de la información. En Lorenzo Cotino Hueso (ed.), *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías* (p. 131-148). València: Servei de Publicacions de la Universitat de València.

Constitutional Council of Iceland. (2011). *Rules of procedure*. Recuperado con fecha de 23 de marzo de 2012, en http://stjornlagarad.is/english/rules-of-procedure/

Cotino, L. (2005). El voto electrónico o la casa por el tejado: La necesidad de construir la democracia y la participación electrónicas por los cimientos. En Lorenzo Cotino Hueso (Coord.), *Libertades, democracia y gobierno electrónicos* (p. 328-347). Granada: Comares, Colección Sociedad de la Información núm.

Cotino, L. (2007). El débil compromiso normativo por la transparencia y participación electrónicas. Situación actual y posibilidades de futuro. En Lorenzo Cotino Hueso (Coord.), *Democracia, participación y voto a través de las nuevas tecnologías* (p. 35-86). Granada: Comares, Colección Sociedad de la Información núm. 13.

Cotino, L. (2011). Del «deber de publicidad» de Brandeis al «Open Government» de Obama (p. 2). Regulación y control de la información pública a través de las nuevas tecnologías. Ponencia invitada en el Congreso Internacional «La protección de los Derechos Humanos para las Defensorías del Pueblo», 1-3 de junio, AECI – Universidad Alcalá de Henares, recuperado con fecha de 14 de julio de 2011, en http://www.goo.gl/br3rs

Cotino, L. (2011). El Reglamento de la Iniciativa Ciudadana Europea de 2011: Su especial regulación de la recogida de apoyos vía internet y de la protección de datos de los ciudadanos. *Revista de Derecho Político* (81), 323-378.

Cuesta López, V. (2010). The Lisbon Treaty's Provisions on Democratic Principles: A Legal Framework for Participatory Democracy. *European Public Law* 16 (1), 123–138.

De Otto y Pardo, I. (1987). Derecho constitucional: Sistema de fuentes. En Ignacio de Otto y Pardo (2010), *Obras completas* (p. 803-1088). Oviedo: Universidad de Oviedo/Centro de Estudios Políticos y Constitucionales.

Elster, J. (2001). *La democracia deliberativa*. Barcelona: Gedisa.

Guichot, E. (2003). El nuevo derecho europeo de acceso a la información pública. *Revista de Administración Pública* (60), 283-316.

Pedraz, E. (1986). Notas sobre publicidad y proceso. En VV.AA., *El Poder Judicial en el conjunto de los Poderes del Estado y de la Sociedad.* Madrid: Consejo General del Poder Judicial.

Rousseau, J. J. (1978). *El contrato social*. Madrid: Aguilar.

Simón Castellano, P. (2011). Los límites jurídico-constitucionales de la Administración electrónica en España y el Open government. *Revista Aranzadi de Derecho y Nuevas Tecnologías* (27), 67-85.

Subirats, J. (2002). Los dilemas de una relación inevitable: innovación democrática y tecnologías de la información y de la comunicación. En Heriberto Cairo (comp.), *Democracia digital: límites y oportunidades* (p. 89-113). Madrid: Trotta.

Taibo, C. (2011). *Nada será como antes: Sobre el movimiento 15-M*. Madrid: Catarata.

COMUNICACIONES SOBRE PRIVACIDAD

PNR AND SWIFT AGREEMENTS. EXTERNAL RELATIONS OF THE EU ON DATA PROTECTION MATTERS

Cristina Blasi Casagran
European University Institute

ABSTRACT: Since the 9/11 attacks there has been a dramatic increase in measures adopted in order to prevent and to combat international terrorism, which has had an impact on the existing data protection framework within the EU.

This study will focus on the analysis of the international agreements signed between the EU and third countries regarding data transfers. In particular, PNR Agreements as well as the SWIFT Agreements will be examined, and I will also analyse the interconnection between the internal and external dimensions in depth, focusing on their mutual impact.

In order to do this, an analysis and comparison of the current EU-US PNR Agreement, EU-Australia PNR Agreement and EU-Canada PNR Agreement will be carried out first. After, I will study the future European PNR Directive and possible implications for current PNR Agreements.

I will then examine SWIFT and SWIFT II Agreements, paying special attention to the enhanced powers of the EP. At this point, it will be necessary to study the European Terrorist Finance Tracking System project as part of the EU Internal Security Strategy.

Finally, concerning the negotiations recently opened by European Union and the United States on an agreement to protect personal information exchanged in the context of fighting crime and terrorism, I will examine this potential international agreement on data transfers between the EU and the US, and its impact on the rest of international agreements with regard to data protection.

KEYWORDS: Data protection, international agreements, PNR, SWIFT, TFTS.

1. INTRODUCTION

The terrorist attacks on September 11, 2001 led directly to the increased number of measures taken by the US authorities and consisting of the collection, processing and storage of personal data in order to prevent and combat international terrorism. These counter-terrorism measures has had an impact on the existing data protection framework within the EU. In particular, closer cooperation between the US and the EU has become a priority, resulting in frequent dialogue and contact between their respective officials in order to harmonise police, judicial and border control policy matters. Thus, many international agreements on border security and criminal matters have been signed between the EU and third countries since 2001, and data protection has come to occupy a key sticking point of such agreements. Therefore, this study will analyse the international agreements signed between the EU and third countries regarding data transfers, looking in depth at the mutual impact of the internal and external dimensions. In particular, it will examine the PNR Agreements and the SWIFT Agreements.

In order to do so, first, the current EU-US PNR Agreement, EU-Australia PNR Agreement and EU-Canada PNR Agreement will be compared and analysed. Subsequently, but still as part of the first section, I will study the future European PNR Directive and possible implications for current PNR Agreements. Second, I will then examine SWIFT and SWIFT II Agreements, paying special attention to the enhanced powers of the European Parliament (hereinafter, EP). At this point it will be necessary to study the European Terrorist Finance Tracking System (hereinafter, TFTS) project as part of the EU Internal Security Strategy. Finally, I will study the recent negotiations for a new US-EU Framework Agreement on Data Protection, an its impact (if any) on current and future international agreements on data transfers, aiming to harmonise both legal orders in the field of data protection matters.

This study is presented as an attempt to disclouse the great external influences (especially from the US) that the EU has been subject to with regard to counter-terrorist measures since 9/11 attacks. However, before starting the analysis of the existing international agreements on data transfers concluded between the EU and third countries, it is worth summarizing in the next section some key issues on data protection with respect to third countries.

2. KEY ISSUES OF DATA TRANSFERS TO THIRD COUNTRIES

When the European Communities adopted the first Directive on data protection in 1995,[1] its *rationale* was to lay down data transfers among Member States as a result of the internal market established since the Maastricht Treaty. Thus, the free movement of goods, persons, services and capital brought an increasing flow of personal data from one Member State to the other, which needed to be regulated within the European territory.

However, both recent technological progress (with the consolidation of the use of Internet) and current global security measures have had an impact on the processing of personal data. Thus, cross-border flows of personal data soon spread beyond European borders as well as beyond pure commercial interests. Accordingly, the market place has undergone an enormous digitalisation in the last twenty years, in which online purchases have increased significantly. This means that not only companies within the EU process personal data in a commercial transaction, but also industries based outside the European borders can easily collect, process and store data from EU citizens.

Regarding data transfers to third countries, the current[2] Directive of 1995 foresees the possibility of carrying out international transfers for commercial reasons. Yet, considering that before the Treaty of Lisbon only the European Communities were empowered with the legal personality necessary to conclude international agreements, that Directive was the one

1 OJ L 281 , 23/11/1995 P.31-50

2 This is the current EU Data Protection Directive at the time this paper is written. However, proposals for a Regulation and a Directive were launched by the Commission on 25th January 2012, and they are being deliberated upon by the EP. See COM(2012) 10 final and COM(2012) 11/4 draft, 25.01.2012.

used as a legal basis to sign international agreements on data transfers. Regarding the requirements to carry out the international transfer, according to article 25.1 of the Directive 95/46/EC, *«The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection»* (Emphasis my own).

According the paragraph 6 of the same article, the general rule is that the Commission has the competence to decide whether the third country guarantees this adequate level of protection or not.[3] However, in absence of the recognition by the European Commission of such adequacy, Data Protection Authorities (hereinafter, DPAs) can determine that a data transfer to third countries is lawful by implementing art. 26.2 of the Directive 95/46/EC. This provision foresees that *«a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights»*. In that situation, considering that the particular third country does not afford *a priori* an adequate level of data protection, the DPA will require a standard application form before performing the transfer, to which is attached a copy of the agreement between the data exporter and the data importer.[4] In that sense, the Commission Decision 2002/16/EC of 27 December 2001[5] was adopted in order to facilitate the transfer of personal data from a data controller established in the European Union to a processor established in a third country which does not offer adequate level of protection. This Decision was repealed in 2010 by the Decision 2010/87/EC,[6] which updated the standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. This legal framework enabled the Commission to sign the first Passenger Name Record (hereinafter, PNR) Agreement, as will be discussed below.

3. PASSENGER NAME RECORD AGREEMENTS

In response to the 9/11 attacks, US authorities adopted measures that obliged airlines taking off, landing or flying through US territory to turn over all their flight booking and

3 For instance, adequate standards has been recognised by the Commission to Argentina, Canada, Switzerland and US, among others.

4 Grigore-Octav Stan and Georgiana Ghitu. «Cross-Border Transfer of Personal Data. The Example of Romanian Legislation», Chapter 17 of *Personal Data Privacy and Protection in a Surveillance Era. Technologies and Practices.* Edithor: Christina Akrivopoulou & Athanasios Psygkas. IGI Global; Hershey PA (USA) 2010, p.309.

5 OJ L 6, 10.1.2002, p. 52.

6 OJ L 39, 12.2.2010, p. 5-17.

departure data to the US government. This information is referred as «*Passenger Name Record*» (PNR) data.

With respect to EU, the Commission has signed three PNR Agreements to date: one with the US, another with Canada and a third one with Australia. Regarding the EU-US PNR Agreement, it was signed pursuant to Art. 25 of Directive 95/46/EC. This agreement was a direct consequence of a US law adopted in November 2001,[7] under which any airline with flights taking off or landing within the US territory was obliged to provide the Bureau of Customs Border Protection (hereinafter, CBP) with electronic access to their PNR data.[8] The EU, in an effort to avoid conflicts between the US law and the existing EU data protection standards, signed a PNR agreement with the US in 2003. Thus, after the US guaranteed an adequate protection of passenger data,[9] the Community adopted Commission Decision 2004/535/EC[10] and Council Decision 2004/496/EC,[11] necessary to execute the international agreement.

On the subject of the chosen legal basis, as mentioned above, the agreement was based on the Directive 95/46/EC, falling thus under the scope of ex-art. 95 TEC (former first pillar). However, the EP, supported by the European Data Protection Supervisor (hereinafter, EDPS), appealed that the Decisions be annulled before the CJEU. The EP argued that the EU-US PNR Agreement had been adopted under the wrong legal basis since it was not an issue concerning an internal market, but rather a matter of public security and criminal law (third pillar). The Court agreed, and in May 2006, annuled both Decisions because it was found that the matter related closer to public security than commercial activity.[12] To explain its ruling, the Court opined *«While the view may rightly be taken that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community law, namely sale of an aeroplane ticket which provides entitlement to a supply of services, the data processing which is taken into account in the decision on adequacy is, however, quite different in nature.[...][T]hat decision concerns not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes».*[13] Consequently, the agreement was annulled as well.

Thereafter, a second PNR Agreement[14] was adopted in October 2006, although it was only provisional. This time the agreement fell under the scope of the third pillar and was

7 U.S. Aviation and Transportation Security Act, Pub.L. 107–71, 115 STAT. 597, 19.11.2001

8 Aviation and Transportation Security Act (ATSA), 19 November 2001 (Public Law 107-71, 107th Congress, 49 USC Section 44909(c) (3) (2001))

9 Undertakings of the Department of Homeland Security, Customs and Border Protection. Retrieved from http://www.dhs.gov/interweb/assetlibrary/CBP- DHS_PNRUndertakings5-25-04.pdf

10 OJ L235, 06.07.2004, p.11.

11 OJ L183, 20.05.2004, p.83.

12 C-317/04 , 30.05.2006. OJ C 178, 29.07.2006, P.1

13 *Ibid*. par.57

14 OJ L 298, 27.10.2006, p. 29-31.

concluded between the EU and the US, culminating with the Council Decision 2006/729/CFSP/JHA.[15] As noted above, international agreements on data transfers signed under the basis of the first pillar had to comply with the «adequacy principle» (Art. 25 Directive 95/46/EC) .This was not the case, however, when they fell under the scope of the third pillar, where each Member State applied its own standards. Therefore, while airline companies' concerns of infringing data protection legislation were solved with this new agreement; new concerns arose within the EU, since the new agreement did not require «adequate» data protection in international transfers.

Regarding the question of who carried out the negotiations, the former art. 24.1 TEU established that, *«When it is necessary to conclude an agreement with one or more States or international organisations in implementation of this title the Council may authorise the Presidency, assisted by the Commission as appropriate, to open negotiations to that effect.»* The Council thus decided on a mandate for the negotiations and authorised the Presidency and the Commission to negotiate on behalf of the EU.[16]

The second PNR Agreement expired on 31 July 2007 and was immediately replaced by the third and current[17] EU-US PNR Agreement.[18] This third Agreement was signed and provisionally applied in July 2007 through the Council Decision 2007/551/CFSP/JHA.[19] However, it has never been formally concluded because of the position of the EP,[20] which has never given its consent to the proposal of the Agreement drafted by the Commission.[21]

The entry into force of the Treaty of Lisbon has given new competences to the EP, which is now required to give consent before concluding any international agreement, according to Article 218 (6) TFEU. Hence, in May 2010, the EP responded to the request on the existing PNR agreement with the US postponing its vote because the agreements did not meet the minimum requirements on data protection.[22] This fact made it necessary to draft a new PNR Agreement between the EU and the US, which was proposed by the Commission

15 Council Decision on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, 13226/06, 11.10.2006.

16 EU/US Passenger Name Record (PNR) Agreement, House of Lords, European Union Committee, 21st Report of Session 2006–07 p.27.

17 At the time this article is written, this is the current agreement. However, a new PNR agreement is expected to come into force in the coming months.

18 OJ L 204, 4.8.2007, p.18-25.

19 OJ L 204, 4.8.2007, p.16-17.

20 European Parliament resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada, P7_TA(2010)0144.

21 COM(2009)702 final, 17.12.2009.

22 P7_TA(2010)0144, 05.05.2010.

in November 2011,[23] and was approved by the EP[24] and the Council[25] in April 2012. The agreement will most likely enter into force in the coming month.[26]

However, as mentioned above, the PNR agreement between the EU and the US was the first but not the only one. In fact, the EU has also PNR agreements with Australia and Canada, and the number of PNR ageeements might increase in a near future, since bilateral negotiations on new PNR agreements with other third countries are currently ongoing. Therefore, it is essential that all these PNR agreements are consistent among them; yet, comparing the three existing PNR agreements, many divergences between them can be noted, as will be analysed below.

First, let us look at the number of data elements requested from the airline companies. The EU-US PNR Agreement (hereinafter, US PNR) offers the most reduced amount of data collected with an attached list of 18 different items. This list has one less data element than the 2007 PNR agreement and definitely much less than the 34-element list included in the first PNR agreement between the EU and the US, in 2004.

The 18-element list in US PNR is also lower than the list of 25 elements annexed in the EU-Canada PNR Agreement[27] (hereinafter, Canada PNR), which was launched in 2005 but never adopted. Likewise, the US PNR has one fewer elements than the new EU-Australia PNR Agreement[28] (hereinafter, Australia PNR), which as in its first agreement with the EU in 2008, has maintained the number of requested elements at 19.

Concerning the data retention periods, the US PNR keeps passenger data the longest, with a retention period of 10 to 15 years (15 years only in the case of terrorists). However, the US authorities justify such a long period by stating that data would only be available in an active database for the first six months, removing afterwards all names, so that data become «depersonalised» by five years. After five years, data would be transferred to a «dormant database», and there kept up to 10-15 years from its collection. In contrast, Canada PNR foresees a retention period of three and a half years, which could be increased up to six years if a person is under investigation. The Australia PNR establishes a period of five and a half years, which ultimately is the same time span stipulated in its first PNR agreement in 2008, albeit that agreement set out a period of retention of three and a half years, with the possibility to extend it two further years when necessary.

---

23 COM/2011/0807, 23.11.2011.

24 P7_TA-PROV(2012)0134, 19.04.2012.

25 9186/12, PRESSE 173, 26.04.2012.

26 *Ibid.*

27 OJ L 82, 21.3.2006, p.15; Adequacy Decision: OJ L 91, 29.3.2006, p. 49.

28 Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, 10093/11, 13.09.2011.
http://europa.eu/rapid/pressReleasesAction.do?reference=PRES/11/324&format=HTML&aged=0&language=EN&guiLanguage=fr

Finally, with regard to the transfer method used, the three PNR agreements prescribe the «push method», a process by which airline companies collect PNR data in their databases and then transfer such data to the respective government authorities. The push system is a sign of progress in respecting data protection rights, considering that in the first and second US PNR Agreements (2004 and 2006) the transfer method was always based on the «pull method». Under the old pull method, the US authorities had access to all data in airline companies' databases; consequently, data was collected and processed under US law, with no regard for EU data protection law. This practice changed with the US PNR in 2007, which made the pull method the alternative when a push method was not possible. With the push method in force, this now means that the processing of data is collected by EU airlines first (which later will be transferred to US authorities) must be in full compliance with the EU data protection legislation. Canada, on the other hand, applied a push method from the beginning, in its first PNR agreement in 2005; and even though Australia did not define it clearly in its first agreement of 2008,[29] the push method is expressly stated in its current PNR agreement with the EU, in force since 2011.

Parallel to the current divergence among the EU PNR agreements with third countries, the EU has launched a proposal for a EU PNR Directive. With this proposal the EU aims to regulate PNR data according to the EU legal framework. The next section discusses the scope and purposes of this Directive.

4. EU PNR DIRECTIVE

Some MEPs have been voicing their concern about the lack of reciprocity on PNR matters: with these international agreements data flows are basically transferred from the EU to the US, but not vice versa. Therefore, along with the negotiation of PNR Agreements, the possibility to create a PNR scheme within the EU has been under discussion since 2007, when the Commission launched a Proposal for a Council framework Decision[30] with the aim to «*harmonise Member State's provisions on obligations for air carriers operating flights to or from the territory of at least one Member State regarding the transmission of PNR data to the competent authorities for the purpose of preventing and fighting terrorist offences and organised crime.*»

More than three years later, in February 2011, the Commission presented a Proposal for a PNR Directive to be adopted by the EP together with the Council,[31] this time under the legal basis of the Treaty of Lisbon,[32] which enhances the competences of the European

29 Agreement between Australia and the EU on the processing and transfer of the EU-sourced Passenger Name Record data by air carriers to the Australian costumes services, 30.06.2008 (OJ L 213, 8,82008, p.49).

30 COM(2007) 654 final, 06.11.2007.

31 COM(2011) 32 final, 2.2.2011.

32 Articles 82(1)(d) and 87(2)(a) TFEU.

institutions. Thus, the Commission stated that the Proposal of Directive was in line with art. 8 of the Charter of Fundamental Rights and the art.16 TFEU, along with the Council Framework Decision 2008/977/JHA.[33]

The proposal was divided into two parts: An explanatory memorandum, where the Commission pointed out the grounds and context and development for the Proposal; and the Proposal as it should be adopted by the EP and the Council, containing twenty articles vis-à-vis the rules concerning PNR transfers.

In the memorandum, the Commission introduced the objective of its Proposal noting the aim of creating a European area of freedom, security and justice and stressing the necessity to establish a harmonised scheme to collect PNR data among EU Member states. The Commission based its Proposal on the recent increase of transnational terrorism as well as the impact of current measures on programmes such as SIS, SIS II, VIS and the Stockholm Programme. Subsequently, the Commission referred to the existing provisions within the EU as border management tools, API, SIS and VIS, highlighting that there would be no interference with the current border controls within the EU, since PNR data is *«used as a criminal intelligence tool rather than as a border control tool»*. The Commission also noted coherence between the Proposal and the Communication of 21 September 2010 'On the global approach to transfers of Passenger Name Record (PNR) data to third countries'.

Regarding the contents of the Proposal of the Directive, its purposes are the prevention, detection, investigation and prosecution of terrorist offences, serious crimes,[34] and serious transnational crimes. In this sense, the Commission put forward a retention of 19 different PNR data for period of time not exceeding five years, although the data must be «anonymised» after a very short period of 30 days. The Commission also emphasises that *«The collection and use of sensitive data directly or indirectly revealing a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life, is prohibited»*.

As in all existing PNR agreements, the Proposal suggests a push method (and not a pull method), in which Member States would not have direct access to the carriers' IT Systems. The text also suggested the establishment of an independent national supervisory authority responsible for advising and monitoring how PNR data is processed as well as a national Passenger Information Unit (PIU) to protect data, which latter would deal with statistical information on PNR data (art. 18 of the Proposal).

Art. 8 of the Proposal is of particular interest, since it foresees that a Member State may only transfer PNR data and the results of the processing of PNR data to a third country on a case-by-case basis. This requirement would be in accordance with the recent PNR Agre-

33 *Op.cit.* COM(2011) 32 final, p.8.

34 Pursuant to Article 2(2) of Council Framework Decision 2002/584/JHA, punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State

ement with Australia (Art. 19.1 of the Agreement), whereas the EU-US PNR Agreement does not mention any case-by-case requirement in its Article 17 on «Onward Transfer».

It remains to be seen what will happen with this PNR Directive, and whether it will finally be approved by the Council and the Parliament. It was proposed by the Commission in February 2011, but no, more than one year later it is still stuck in the EP. In contrast, the EU-US PNR Agreement was proposed eight months later, and EP has already voted in favor of it. it has already been voted by the EP. Hence, it seems that an agreement on the external PNR schemes was foregoing the internal dimension of the EU PNR Directive.

Moreover, it is presently an open question regarding how the existing PNR internacional agreements will interact with the Directive. In this respect, if the Directive is finally adopted as it is proposed today, it could produce at least two results for passengers that fly from Europe to the US: i) such passenger would have 18 PNR collection items transferred to the US, but 19 in the EU database; or ii) such collected passenger PNR data would be retained for 15 years in the US and only 5 years in the EU.

Lastly, despite the new PNR Directive having the objective of preventing 27 divergent national systems,[35] it could paradoxically create additional fragmentation between EU data protection laws and those in third countries. Consequently, the mutual impact between the internal and external PNR regulatory frameworks will be of a greater interest in the times ahead, as such impact could determine the EU's position and level of influence regarding data processing matters.

5. SWIFT AGREEMENTS

Since September 11, 2001, there has been exchange of financial data between the US and the EU. In fact, in December 2001, two US – Europol agreements were concluded to facilitate the exchange of information related to global financial movements.[36] They were part of the so-called Terrorist Finance Tracking Program (hereinafter, TFTP), originally a secret Program uncovered in 2006 by the New York Times.[37] The Program, which was created by the Bush administration after the 9/11 attacks as an antiterrorist measure, in the beginning consisted in the US authorities pulling data from the private company *Society for the Worldwide Interbank Financial Telecommunication* (hereinafter, SWIFT) on EU citizens, without any involvement

35 Some Members States, such as UK or Belgium, have already their own PNR systems.

36 «Agreement Between the United States of America and the European Police Office», December 6, 2001, at https://www.europol.europa.eu/sites/default/files/flags/united_states_of_america.pdf; «Supplemental Agreement Between the Europol Police Office and the United States of America on the Exchange of Personal Data and Related Information,» December 20, 2002. https://www.europol.europa.eu/sites/default/files/flags/supplemental_agreement_between_europol_and_the_usa_on_exchange_of_personal_data_and_related_information.pdf

37 Eric Lichtblau and James Risen, «Bank Data Is Sifted by U.S. in Secret to Block Terror», *The New York Times*, June 23, 2006. http://www.nytimes.com/2006/06/23/washington/23intel.html?pagewanted=all

of the EU, since this company was based in Belgium but had servers located in US territory. Even though SWIFT had to comply with Belgian national law implementing Directive 95/46/EC (first pillar), in order to avoid potential clashes of its practices with the European law, the company always processed EU citizens' data through its servers located in the US. Later, however, the fact that SWIFT servers moved completely to European territory[38] made impossible to avoid European privacy concerns, and the Commission urged to draft an Agreement enabling such data transfers from the EU to the US, because it was clear that the purpose of this cross-border transfer was not commercial but for criminal matters.

Consequently, on 30 November 2009, under the legal basis of the former Art. 24 and Art. 38 TEU, the EU and the US signed the first official SWIFT Agreement, exactly one day before the Lisbon Treaty came into force. This event had important consequences.[39] The agreement was provisionally applied on 1 February 2010 and was supposed to be applied temporarily until 31st December that same year. However, the legal basis to conclude international agreements changed with the Treaty of Lisbon and so too did the powers of the EP: From the Treaty of Lisbon, the Council can only adopt a decision authorising the conclusion of the agreement after obtaining the consent of the EP.[40] Thus, on 11 February 2010, the EP rejected the adoption of SWIFT Agreement, arguing a lack of protection of personal data.[41] After the EP withheld its consent with regard to SWIFT, the Commission received a mandate by the Council to restart negotiations with the US authorities with the aim of composing a new draft agreement (SWIFT II).[42] The new text was approved for a five-year period by the Council and this time also by the EP in July 2010.[43]

Nevertheless, even this new SWIFT agreement between the EU and the US has been controversial. The EDPS pointed out in an Opinion[44] that the bulk transfer of personal data should be replaced by a filtering mechanism in the EU, transferring only relevant and necessary data to the US and that the retention period of five years was too long. Likewise, the EP[45] raised concerns in March 2011, since Europol, which is in charge of checking US

38 Marise Cremona, « Justice and Home Affaires in a Globalised World: Ambitions and Reality in the tale of US-EU SWIFT Agreement», *Institute for European Integration Research,* Working Paper nº 04/2011, Viena, p.13; and Deirdre Curtin «Top Secret Europe», *Universiteit vvan Amsterdam*,p.6.

39 For a more exhaustive analysis of the facts, see, Cremona M, « Justice and Home Affaires in a Globalised World: Ambitions and Reality in the tale of US-EU SWIFT Agreement», *Institute for European Integration Research,* Working Paper nº 04/2011, Viena., 11-13; and Curtin D. M, «Top Secret Europe», *Universiteit vvan Amsterdam*, 2011.

40 Article 218 (6) TFEU.

41 P7_TA(2010)0029.

42 Council of the European Union, 11575/10 PRESSE 194, 28.06.2010.

43 A7-0224/2010, 05.07.2010.

44 OJ C 355, 29.12.2010, p.10.

45 Press release, «SWIFT implementation report: MEPs raise serious data protection concerns», Committee on Civil Liberties, Justice and Home Affairs, March 2011.

compliance with the agreement, did not provide any updated-written information about the requests from the US Treasury Department and its compliance with European data data protection standards. The dispute on document secrecy between the Council and the EP ended up on 4 May 2012 when the CJEU ruled in favour of the EP document requests[46]. The Council argument about the «negatively impact on the European Union's negotiating position» did not convince the Court, since the Council had «not established the risk of a threat to the public interest». Thus, the CJEU decision will probably increase the EU transparency rules in the negotiation of international agreements[47].

Moreover, as in PNR schemes, the interdependence of internal and external objectives[48] on data processing within the scope of the AFSJ had an impact on the subsequent data protection legislation within the EU with regard to financial data, as will be examined in the next section.

6. CREATION OF EU TFTS

The SWIFT II Agreement included two additional changes. The first was Commission's appointment of an independent observer based in Washington D.C., and the second was the future creation of an EU program equivalent to the US TFTP.

Considering this last condition, the EU is currently negotiating its own European Terrorist Finance Tracking System (hereinafter, TFTS), which would run parallel to the current US TFTP. In July 2011, the Commission launched a Communication called «A European terrorist finance tracking system: available options».[49] In it the Commission pointed out that *«the possible establishment of a system for extracting the data on EU territory would have consequences for the existing EU-US TFTP Agreement…[which] would need to be adjusted if the European Union decides to establish such a system.»* According to art. 72 TFEU, which states that the EU cannot affect the responsibility of its Member States on issues regarding «*the maintenance of law and order and the safeguarding of internal security»,* the Communication contained different available options for the EU and its TFTS,[50] which will have to be debated by the Council and the EP. In particular, the Commission proposed three possible TFTS. In the three of them the safeguards and controls would be centralised, but data pro-

46 T-529/09 - In 't Veld v Council, 04.05.2012.

47 FOX, B (2012), «Commission pushes for document secrecy despite court judgement», *EUObserver.com,* 08.05.2012. Retrieved from http://euobserver.com/22/116181

48 CREMONA M (2011) «The External Action in the JHA Domain: A Legal Perspective» in *The External Dimension of the Area of Freedom, Security and Justice*, ed. M. Cremona, J. Monar, S. Poli (Brussels: Peter Lang, 2011), 6.

49 COM(2011) 429 final, 13.7.2011.

50 The first option would be the creation of a EU TFTS coordination and analytical service, the second an EU TFTS extradition service, and the third would be a Financial Intelligence Unit coordination.

viders are still undefined, since it would probably include many companies and not only SWIFT, unlike the current SWIFT Agreement.

Moreover, the Commission is unclear about whether it would be more convenient to establish the system in the form of an «EU central TFTS Unit» or, instead, a Financial Intelligence Unit (FIU) Platform. The latter would suppose a higher involvement of the Member States, since this platform would be composed of all FIUs of Member States.

Furthermore, the Commission leaves open the role of this system, proposing three different options: The first would consist of managing the search results, so that the requests would be at a EU level; on the contrary, the system could also have a more limited role, only distributing searches to the Member States, which would be the ones in charge of the requests; and finally the Commission foresees, in the case of the FIU Platform, the possibility of handling citizens' requests as well as conducting searches. These searches would be verified either at the national or the EU level.

In addition, it is not yet clear whether the key bodies of the system would be the current Europol[51] and Eurojust, or, in the case of the FIU Platform, FIUs and national authorities would constitute the institutional structure. Finally, the legal basis for this EU TFTS is still undefined, but it would not be surprising that it is the same proposed in the PNR Directive, namely, Art. 82(1)(d) and Art. 87(2)(a) TFEU.

Whatever the scope and nature of this system turns out to be, the Commission points out that it is to be seen as positive, since it would contribute to limiting the amount of personal data transferred to the US (limiting the transfer of bulk data to the US). Nevertheless, the Art. 29 WP reacted against this Communication in September 2011,[52] saying that it is not entirely clear how this aim of limiting the data to be transferred would be met. In particular the Art.29 WP noted that the Communication refers to collection of the so-called «raw data», which in fact, if the data minimisation principle is not complied with, could be considered as «bulk data». Moreover, the Art. 29 WP argues that there is no evidence that the processing of personal data with regard to the EU TFTP is necessary, proportionate and legitimate as a remedy for the shortcomings of current US-TFTP.

Likewise, this EU TFTS project, as part of the EU Internal Security Strategy, is presented by the Commission as an attempt to prevent the transnational transfer of certain data belonging to European citizens to US authorities, so that the external regulation of collection and storage of financial data according to SWIFT II will have to be adapted to this new EU framework, constraining the collection and transfer of data according to the levels

51 However, the EDPS (Opinion June 2010), the EP (Press release March 2011) and the Art. 29 WP (Letter September 2011) have already raised concerns about the independence of Europol in the processing and transfer of personal data.

52 Letter from Article 29 Data Protection Working Party to Commissioner Cecilia Malmström. Subject: Terrorist Finance Tracking System (TFTS) – European Commission Communication COM (2011) 429. 29.09.2011.

of necessity and proportionality. However, the Art. 29 WP has already stated that it will be difficult to continue the existing US-TFTP parallel with the establishment of the EU TFTS.

Finally, as with the above-mentioned future impact between the EU PNR Directive and the current PNR agreements, the compatibility of the EU TFTP with the SWIFT II Agreement will be of great importance. Will this European program follow the existing external scheme on financial data transfers? Or rather, will the European model establish the parameters to amend the current SWIFT agreement? It is still too early to answer this question; however, if the future EU TFTS has a stronger impact on the SWIFT II, it could solve the current lack of transparence in the transfers to the US territory. Additionally, it could offer higher data protection standards when EU financial data is transfered beyond European borders.

7. STEPS FOR THE US-EU FRAMEWORK AGREEMENT ON DATA PROTECTION

As the number of international agreements on data transfers between the EU and the US has increased significantly in the last ten years, many attempts have been made to reach a general adequacy framework on data protection between them. However, while Washington wants an umbrella agreement in which the EU would largely accept US data privacy standards as adequate, and thereby making the negotiation of future data-sharing accords easier,[53] the EU is willing to make the US amend its privacy laws so that they comport with the EU data protection legal framework.

The EP launched the first call for this agreement in March 2009.[54] One year later, in May 2010, the Commission drafted a mandate on the negotiation terms,[55] which the Council authorised on 3 December 2010.[56] Negotiations officially commenced in March 2011.[57] Since then, several meetings have taken place between the Commission and the US authorities.[58] Furthermore, in November 2011, the EU and the US pledged in a joint statement to finalize negotiations on a comprehensive US-EU data privacy and protection agreement.[59]

---

53 Kristin Archick, *«U.S.-EU Cooperation Against Terrorism»*, Congressional Research Service, May 2, 2011, p.10.

54 OJ C 117 E, 6.5.2010, p.198-206.

55 IP/10/609.

56 See Commission press release on http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1661.

57 MEMO/11/203, 29.03.2011.

58 To date, sessions have been held on 5-6 May, 26 May, 24 June, 28 July, 9 September, 9 November, 13 December 2011 and 13 February 2012. See European Commission, JUST/C3/MHB D(2011), 31.01.2012.

59 MEMO/11/842, 28.11.2012. The same idea was also reminded in MEMO/12/192, 12.03.2012.

With regard to the content of the agreement, the US authorities have been leading the negotiations, highlighting their preferences in terms of data retention, «transfers onwards», data breach notification, sensitive data, and liability and proportionality rules. In this respect, the US has taken a position against establishing specific data retention periods, suggesting that such periods should be decided in accordance with each parties´ domestic law.[60] As regards data breach notifications, the US considers that only *serious* breaches should be notified, while the Commission has supported the notification of data breaches in all cases, excluding certain exemptions.[61] In addition, the US appears reluctant to transpose the High Level Contact Group's (HLCG) principle of *proportionality*[62] in the agreement, arguing that this term is foreign to US data protection law, and that such a principle could produce unknown effects.[63] Finally, the Commission is pushing to get that individuals have a real possibility to obtain administrative and judicial redress, establishing enforceable legal provisions.[64]

Although the EU and the US view the Agreement´s adoption as a long-term goal, the truth is that it is currently taking shape at a time where many changes are occurring in the area of data processing. In particular, there have been recent moves from both the US and the EU legal orders in order to align their data protection in some respects. For instance, on 25 January 2012 the Commission proposed a European Data Protection Package, composed of a General Data Protection Regulation and a Police and Criminal Justice Data Protection Directive.[65] Later, the White House launched a White Paper on a future «Consumer Privacy Bill of Rights» on 22 February 2012.[66] This Bill lays down the basis for a federal US legal framework on data privacy, which currently falls under sectoral legislations. Only time will tell how a future EU-US data protection agreement will interact with both the US and the EU internal data protection legilations.

On the subject of the material scope of the agreement, it has been agreed by both the Commission and the US authorities that the agreement itself will not be the legal basis for any transfers of personal data, and that a specific legal basis for such transfers will always be required.[67] Consequently, the future general agreement will probably not be prioritised

60 European Commission, JUST/C3/MHB D(2011), 31.01.2012.

61 *Ibid.*

62 About HLCG principles, see http://www.statewatch.org/news/2008/mar/eu-us-dp-principles.pdf

63 JUST/C3/MHB D(2011), Op.cit. For further information about the HLCG, see Mary Ellen Callahan, «New International Privacy Principles for Law Enforcement and Security», retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_new_int_privacy_principles_law_enforcement_security.pdf

64 REDING V, SPEECH/12/316, 3.05.2012, p.8.

65 COM(2012) 10 final and COM(2012) 11/4 draft, 25.01.2012.

66 White House, «Consumer Data Privacy in a Networked World: A Framework for Protecting and Promoting Innovation in the Global Digitally Economy. February 2012. Retrieved from: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

67 European Commission, JUST/C3/MHB D(2011), 31.01.2012.

over other more specific EU-US international treaties dealing with data processing matters. Moreover, the US has already stated that the new agreement will not be applicable to cases where data are collected by private parties and afterwards processed by law enforcement authorities for security purposes.[68] In PNR and SWIFT agreements the private parties involved (i.e., air carriers and the Belgian bank SWIFT) collect personal data for EU internal market purposes, but then, they transfer them to the US authorities for preventing and combating terrorism. Accordingly, the impact of this future agreement on current PNR and SWIFT agreements with the US might be very small (or even non-existent).

Thus, only at first sight the future US-EU data protection agreement could result in the most successful legislative tool for establishing common minimal standards on data protection between both the EU and US. However, the fact that the US has already constrained the scope of the Agreement to specific law enforcement purposes makes one wonder what the real impact of the Agreement will be.

8. CONCLUSION

From the foregoing discussion, we can see that there has been a clear evolution regarding the European external competence to legislate data protection. Originally, the Community was competent, enjoying implied powers to negotiate internal market issues beyond the European borders.[69] However, the increase of international terrorism has compelled the EU to adopt new international agreements on data transfers such as PNR Agreements and SWIFT Agreements. Thus, since the 9/11 attacks and the terrorist attacks in Madrid and London in 2004 and 2005, there has been a progressive shift in the purposes of processing personal data from the commercial reasons (former first pillar) to the aim to adopt criminal measures (former third pillar). This has had implications for the applicable legal basis to conclude international agreements, since it was no longer the Community that was competent to conclude international agreements on data flows regarding criminal matters, but the EU.

At the same time, these new international agreements have pushed the EU to amend its own internal legislation on data protection, in order to solve the problems of legal basis stemming from the confusing structure in pillars and its blurred division depending on whether the purpose of processing data is commercial or for security reasons.

Given the prevalence of these PNR and SWIFT agreements, it is clear that the EU security policy could benefit from additional structural coherence between its internal and external aspects. Not only have there been divergences, but fragmentations concerning data protection laws have also occured among EU Member States, as well as between the EU and other third countries. In response to these controversies, since the Treaty of Lisbon the protection of personal data in the EU has enjoyed unprecedented status, which has been

68 *Ibid.*

69 Following ERTA-Doctrine.

reflected through subsequent proposals by the Commission: the EU PNR Directive and the EU TFTS. Both proposals aim to legislate *internally* issues that have already been legislated *externally* for years.

Moreover, in seeking to strike the balance between the protection of personal data, on the one hand, and data processing for security purposes, on the other, the EU and the US are considering the adoption of a EU-US data protection agreement. However, so far it is difficult to see what impact this future umbrella agreement will have on the existing EU-US deals, such as PNR and SWIFT. Although the future EU-US data protection agreement is announced as an attempt to bring the European and American legal orders closer, it is unclear what the scope and implications of this agreement will be.

Regarding the interplay between the European and international perspectives in terms of data processing, to date the US legislation has undoubtly been the main influence on EU internal legislation and international agreements on this field. It is true that the European institutions (especially the EP) have been leading the promotion of individual data protection; yet, necessity and the external pressures for the EU to cooperate in a transatlantic counter-terrorism framework are too strong. Hence, as it has been recently seen with the EP aproval of the new EU-US PNR Agreement, the EU, in some cases, is willing to prioritise security over the EU fundamental right of data protection.

9. BIBLIOGRAPHY

Cremona M. (2011) «The External Action in the JHA Domain: A Legal Perspective» in *The External Dimension of the Area of Freedom, Security and Justice*, ed. M. Cremona, J. Monar, S. Poli (Brussels: Peter Lang).

Callahan M.E (2010) «New International Privacy Principles for Law Enforcement and Security», *The Privacy Advisor,* The Official Newsletter of the International Association of Privacy Professionals (IAPP), January 2010 Retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_new_int_privacy_principles_law_enforcement_security.pdf

Cremona M. (2011), « Justice and Home Affaires in a Globalised World: Ambitions and Reality in the tale of US-EU SWIFT Agreement», *Institute for European Integration Research,* Working Paper nº 04/2011, Viena

Cremona M. (2010), «Disconnection Clauses in EC Law and Practice» in *Mixed Agreements Revisited - The EU and its Member States in the World*, eds. C Hillion and P Koutrakos (Oxfort: Hart Publishing, 2010).

Curtin D. M (2011) «Top Secret Europe», *Universiteit vvan Amsterdam*.

Laja S. (2012), *UK joins EU deal to share air travellers' data with US*, TheGuardian, 01.03.2012. Retrieved from http://www.guardian.co.uk/government-computing-network/2012/mar/01/home-office-pnr-agreement-eu-us?INTCMP=SRCH

Lichtblau E., Risen J. (2006), «Bank Data Is Sifted by U.S. in Secret to Block Terror», *The New York Times*, June 23, 2006. Retrieved from

http://www.nytimes.com/2006/06/23/washington/23intel.html?pagewanted=all

Pérez Francesch J.LL, Gil Márquez T. and Gacitúa Espósito, A. (2011) «Informe sobre el PNR. La utilización de datos personales contenidos en el registro de nombres de pasajeros: ¿fines represeivos o preventivos?» Institut de Ciències Polítiques i Socials, UAB. Working Paper 297, Barcelona.

Reding V. (2011) «Stronger data protection rules at EU level: EU- Justice Commissioner Viviane Reding and German Consumer Protection Minister Ilse Aigner join forces», MEMO/11/762, November 07, 2011.

Reding V. (2011) «Building trust in the Digital Single Market: Reforming the EU's data protection rules», SPEECH/11/814, November 28, 2011.

Stan, G.O. and Ghitu, G. (2010), «Cross-Border Transfer of Personal Data. The Example of Romanian Legislation», Chapter 17 of *Personal Data Privacy and Protection in a Surveillance Era. Technologies and Practices.* Edithor: Christina Akrivopoulou & Athanasios Psygkas. IGI Global; Hershey PA (USA).

Worth D. (2011) *EC wants all non-European business to adhere to Data Protection Directive*, v3.co.uk, November 08, 2011. Retrieved from http://www.v3.co.uk

ONLINE ENTERTAINMENT IN CLOUD COMPUTING SURROUNDINGS

Philipp E. Fischer
Sui Generis Consulting (CEO), Munich
Data Protection Officer & - Auditor (TÜV)
IT Lawyer. LL.M. (London/Dresden)

Rafael Ferraz Vazquez
Veirano Advogados, Rio de Janeiro
Media & Entertainment Lawyer
LL.M. in IP (Alicante)

ABSTRACT: Modern companies in online entertainment businesses generate masses of digital information every day and store such data in order to maintain and improve their services. Their quotidian major business processes have created a challenging level of technological complexity and interdependencies, especially if companies store data centralized in cloud computing services. Deep in this whirlpool of data flow, personal data can be found and privacy concerns do arise.

The authors will give one key example: The social media plugin, which allows internet users to express their appreciation of something online. Germany recently banned the use of Facebook´s like button on websites in certain regions. This was introduced specifically to prevent user data being sent without any user consent to U.S.-based servers with the result of tracking users from website to website. Other countries and its Data Protection Authorities also started to pay attention on such plugins.

Thus, storm clouds are forming around the topic of privacy in the cloud. Aiming at the maintenance of Online Entertainment Services (OES) – how can privacy legislation and enforcement be improved at the same time in order to set juridical limits to data streams being as free as never before? On the other hand: Of course privacy is an important issue - but should it encroach on what makes the Internet so good?

KEYWORDS: Online entertainment, social networking services, privacy, data protection, cloud computing, international data transfer, European Data Protection Directive, privacy by design, user generated content, social plugins, like button, facebook, youtube, terms and conditions, controller, processor, data subject, personal data.

1. INTRODUCTION

During the last IT-fair «Cebit» this month in Hannover, René Obermann, CEO of Deutsche Telekom, highlighted that «the present PC-architecture is outdated, the Post-PC-era has begun. […] We want to play an important role in the ecosystem cloud»[1]. Not surprisingly, because Germany´s BITKOM[2] association lately issued a study, finding that the annual turnover

1 Die Welt, «Die Post-PC-Ära hat begonnen», 6 March 2012, p. 11

2 http://www.bitkom.org/

in cloud computing businesses in Germany will end up around 5.3 Billion Euros in 2012, a steep increase of 50% compared with the previous year, the prediction for 2016 is even about 17 Billion Euros per year, a third of it through business to private consumer relations. Market analysts recently determined the global returns of cloud computing in 2012: 77 Billion Euros.[3]

Big market players such as Google, Facebook & Co. collect vast amounts of personal data through their services and transfer it into the cloud. The most recent example for this is the use of so-called social plugins. The most widely used among social plugins is still undisputedly Facebook´s like button[4]. He was used on more than 50,000 websites back in April 2010, and now on more than 2.5 million Web pages[5], on which worldwide website visitors' click at an average of 50 million times a day[6]. According to a study by the Wall Street Journal[7], the like button is more diligent in collecting data than a traditional cookie, so its function is basically «like a tracking tool.» This fact leads to a large number of potentially affected data protection laws and is therefore highly questionable.

Hence, Data Protection Authorities (DPAs) started to take action against Facebook in 2011. The Hamburg City Council decided to take social plugins down from its website[8]. A few weeks later, the Independent Centre for Data Protection (ULD), the data protection supervisory authority for companies in the German federal state of Schleswig-Holstein, found that the use of a like button is illegal and called on site operators to remove it[9].

Since then, the ULD and other DPAs are constantly in dialogue with Facebook. The ULD says it will not give up hope that someday Facebook-applications will be designed and used in compliance with data protection and privacy.

This shady side of new opportunities through cloud computing has been addressed not only by Germany´s chancellor Angela Merkel: «The more natural technologies become, the more important is the necessity of trust.»[10] Viviane Reding, Commissioner of the European Union (E.U.) illustrated: «Let's take cloud computing: storing information in the cloud holds much economic promise and many consumer benefits. Cloud computing is becoming one of the backbones of our digital future. However, new technologies also raise challenges for policy makers. A cloud without robust data protection rules is not the sort of cloud we need»[11] and

3 Frankfurter Allgemeine Zeitung (F.A.Z.), 4 March 2012

4 http://www.brightedge.com/socialshare

5 http://fbwatchblog.de/facebook-like-button-auf-25-millionen-websites-08052011

6 http://fbwatchblog.de/facebook-nutzer-klicken-50-mio-mal-taeglich-auf-gefaellt-mir-25052011

7 http://professional.wsj.com/article/SB10001424052748704281504576329441432995616.html?mod=rss_Technology&mg=reno-secaucus-wsj

8 http://intern.hamburg.de/2010/06/22/wieso-wir-den-facebook-like-button-wieder-entfernten/

9 https://www.datenschutzzentrum.de/presse/20110819-facebook.htm

10 speech of *Angela Merkel* at the Cebit fair, F.A.Z., 6 March 2012

11 Viviane Reding, «Privacy standards in the digital economy: enhancing trust and legal certainty in transatlantic relations», 23 March 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/210

«privacy nowadays has become a moving target: new risks need better legal remedies.» [12]

In a globalized online entertainment world, the free data flow and use of OES became an everyday need. A formula has to be found to make sure that privacy in the cloud does not prejudice these goals and at same time enhances the protection of user´s privacy rights. This is going to be long journey.

In the present article, we analyze the current European data privacy framework in light of new technologies features such as the OES, cloud computing and the upcoming pervasive privacy in user's communication tools. In light of this new environment regarding private data, we will approach the European Union's call for new legislation as well as the employment of technical solutions for the sake of data protection. Some of these solutions, such as Privacy by Design (PbD) might be considered as the only effective solution against this ever-growing volume of processing of private data.

2. ONLINE ENTERTAINMENT- AND CLOUD COMPUTING SERVICES

2.1. Online entertainment services

New possibilities of the internet modified what it is used for. The focus on the internet stopped being on content suppliers[13] and shifted to users, once it is not predominantly a new source of static information available to be accessed. Interactions on Online Entertainment Sites (OES) such as the Social Network Sites (SNS) are the new state-of-the-art. Before, online interactions were pre-defined, such as in an online store where you choose from a list of options. OES on the other hand provide a multiple, free and intense online interaction.

But the new interactions also represent new data protection risk. In recent analysis[14] of the 100 most popular applications of the Facebook it was revealed which information of the user is collected. Surprisingly or not, some applications did not even have a privacy policy implemented! The Research Centre on IT and Law (CRID)[15] pointed out four main risks linked with large public available Web 2.0 platforms:

- Profiling and behavioral advertisement
- Lack of consent from the users
- Ownership and control over the information by the data subject
- Control over the data of diseased data subject.

12 Viviane Reding, «Privacy matters – Why the EU needs new personal data protection rules», 30 November 2010, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700

13 CEPIS, «Social Networks – Problems of security and Data Privacy Statement»

14 The Wall Street Journal, Selling you on Facebook Available on: http://online.wsj.com/article/SB10001424052702303302504577327744009046230.html?mod=googlenews_wsj, Accessed on April 10, 2012.

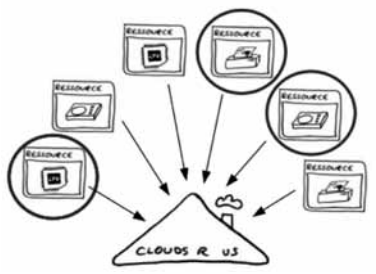
15 Research Centre on IT and Law (CRID), «Cloud Computing and its implications on data protection», Discussion Paper, 2010

While internet users were still impressed and looking for an enhanced Web 2.0 experience, privacy rights were and still are left to a second level of importance by users, service providers and until recently, governments and DPAs.

2.2. Cloud computing services

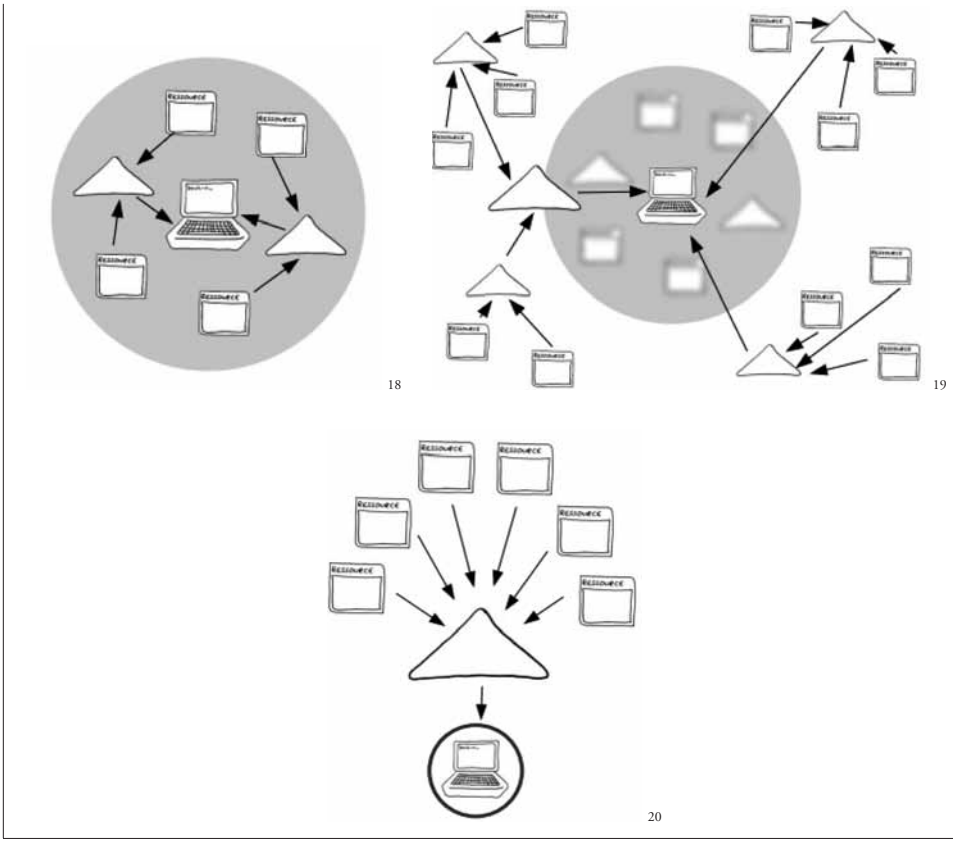
Although cloud computing services have been on offer for many years, the significantly increased use of SNS as Facebook and Google+ in a cloud computing surrounding opened the public debate on «what is cloud computing?» The relevant players in a cloud computing surrounding are:

- resource owner
  A cloud computing model is composed of three service models, depending on the type of resources offered by the resource owner:
  – Infrastructure as a service («Iaas»):
    IT services like hardware components[16].
  – Software as a service («SaaS»):
    Application packages, Email, ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), ECM (Enterprise Content Management).
  – Platform as a service («PaaS»):
  Resources and infrastructure-software, e.g. webserver, databases.



17

- cloud provider
  There are four models for deploying these resources bundled in a cloud computing service:
  – private cloud (image):
    Services are exclusively used by one institution, even if supporting public processes are running in the background. Resource, cloud provider and cloud user are the same entity (e.g. one company).
  – public cloud (image):
    Services can be used by everybody. All physical resources are not owned by the cloud user.
  – hybrid cloud:
    A hybrid cloud mixes elements of both, public and private cloud.
  – community cloud:
    The cloud infrastructure is commonly used by different organizations, which do have their common standards (e.g. security, privacy, compliance) and support a specific community.
- cloud user (image)
  The advantages of cloud computing for the end user are: Anytime and broad network access, hardware cost reduction, efficiency, rapid elasticity, measured service. But it´s key feature is what is called the «scalability» of service, meaning that services and resources can be scaled up or down depending on the users´ demand.



Regarding OES, cloud provider and resource owner are mostly the same entity. For example Facebook uses its own cloud in order to offer web-based application services online to its end users. The cloud user in our case is at the same time an online entertainment end user.

16 as an example on the image from right to left: storage, print, compute

17 *Ina Schiering / Markus Hansen:* Sind Privacy und Compliance im Cloud Computing möglich? Heise-Forum Sicherheit und IT-Recht, CeBIT 2010, 4 March 2010

18 *Ina Schiering / Markus Hansen:* Sind Privacy und Compliance im Cloud Computing möglich? Heise-Forum Sicherheit und IT-Recht, CeBIT 2010, 4 March 2010

19 *Ina Schiering / Markus Hansen:* Sind Privacy und Compliance im Cloud Computing möglich? Heise-Forum Sicherheit und IT-Recht, CeBIT 2010, 4 March 2010

20 *Ina Schiering / Markus Hansen:* Sind Privacy und Compliance im Cloud Computing möglich? Heise-Forum Sicherheit und IT-Recht, CeBIT 2010, 4 March 2010

3. THE CONCEPTS OF PRIVACY AND DATA PROTECTION

The «Article 29 Data Protection Working Party»[21] (A29WP) issued a statement about what is «personal data» in order to clarify the EU-DPD´s approach, divided into four key elements: Any information, relating to, identified or identifiable, natural person.

Within the E.U. the concepts of data protection and privacy are «twins, but not identical»[22], and data protection law «seeks to give rights to individuals in how data identifying them or pertaining to them are processed, and to subject such processing to a defined set of safeguards»[23], while privacy can be seen as a «concept which is broader than data protection, though there can be a significant overlap between the two.»[24]

Thus, the authors of this writing will keep in mind that data protection is one key element within peoples´ privacy rights, the scope of this element goes from protecting their «right to be left alone»[25] until their «right to be forgotten»[26]. Art. 2 (b) EU-DPD provides that «Processing of personal data shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.»

4. INTERFACES BETWEEN CLOUD COMPUTING AND ONLINE ENTERTAINMENT

4.1. Accountability between controller and processor

The concepts of the EU-DPD, once clear and useful, became blur on Web 2.0. As an example, in an OES remains questionable who is data subject, data controller and data processor, not alone the position and duties of those responsible for applications[27] inside OES.

---

21 http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

22 *Paul de Hert / Eric Schreuders*, «The Relevance of Convention 108. European Conference on Data Protection on Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data: present and future», from DP Conf (2001) Reports, p. 63-76, The Council of Europe (ed.), http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/events/conferences/DP%282001%29Proceedings_Warsaw_EN.pdf, p. 42

23 *Christopher Kuner*, «An international legal framework for data protection», p. 308

24 *Christopher Kuner*, «An international legal framework for data protection», p. 309

25 stated already in the 19th century by *Warren / Brandeis*, «The Right to Privacy», Harvard Law Review, Vol. IV No. 5, 15.12.1890, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

26 now addressed by the European Commission during its consultations for the proposal of a comprehensive reform of the EU's 1995 data protection rules, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf.

27 Many successful games are accessible on Facebook, e.g. Mafia Wars and Farmville created by the company Zynga which achieved more than 240 million monthly active users playing its games in

Some issues are only raised when the subscribers are legal entities: how to differentiate user, subscriber and data subject in a corporate environment, scope of protection granted to legal persons, the binding regulations such as duty of secrecy and non-disclosure, and national sovereignty of data from the public administration.

Some of those questions were partially answered by the A29WP in 2009: «SNS providers are data controllers under the Data Protection Directive. They provide the means for the processing of user data and provide all the «basic» services related to user management (e.g. registration and deletion of accounts). SNS providers also determine the use that may be made of user data for advertising and marketing purposes – including advertising provided by third parties.» [28]

The cloud user typically acts as the controller and the cloud service provider as the processor, although in certain cases the cloud service provider may be a controller. In order to allow the cloud user to comply with the rights of data subjects, the data protection authorities recommend, in particular, that the cloud user contractually reserves—subject to penalties—the right to give instructions to the cloud service provider that guarantee the rights of data subjects.

4.2. Ubiquity and different data protection levels

A cloud is by its nature not necessarily tied to any particular location. Such feature is not an exclusivity of the cloud, but rather an upcoming ICT's standard feature. This ubiquity is named pervasive computing, generally categorized in: computing ('devices'), communications ('connectivity') and 'user interfaces'[29]. The result of pervasive computing and it existence is mostly invisible to users once it simultaneously runs a series of processes in the background, turning objects in the real world into part of an information and communications system (the private data). While using the OES, there is almost no knowledge regarding these processes, even though they raise a number of issues with regard to data protection.

While the cloud is ubiquitous, legislation is not. The EU-DPD provides a strict legal regime and high level of data protection. It requires that any country to which European personal data is sent must have an adequate level of data protection as measured by E.U. standards. As many cloud computing providers are based outside the E.U. but wish to conduct their business within the E.U., they must ensure an adequate level of protection. This fact forced U.S. and E.U.to a bilateral convention, the safe harbor agreement. But even within the E.U. different ways of implementing the Directive´s Art. 17 into national laws do exist. The A29WP has been helping in such harmonization but as it seems to be, a European Regulation might be the solution.

SNS such as Facebook, Myspace and Orkut.

28 see Nr.4

29 *Parliament Office of Science and Technology*, «Pervasive Computing», Postnote, N. 263, May 2006.

4.3. Jurisdiction, applicable law and enforcement

4.3.1. Jurisdiction

Robert Gellman of the World Privacy Forum highlighted issues raised by data location: «The European Union´s Data Protection Directive offers an example of the importance of location on legal rights and obligations. Under Article 4 […] Once EU law applies to the personal data, the data remains subject to the law, and the export of that data will thereafter be subject to EU rules limiting transfers to a third country. Once an EU Member States´ data protection law attaches to personal information, there is no clear way to remove the applicability of the law to the data»[30].

At this point, the differentiation between private cloud and public cloud becomes crucial. For a private cloud solution which processes e.g. «German data» –data processed on servers, computers and storage systems exclusively operated in Germany– only German law applies. Thus, a private cloud poses no special problems for international private law (IPL) –as far as the transfer of personal data into a cloud is carried out on German territory. Whenever personal data is processed in a public cloud, it has to be assumed that this data is being processed on computers and storage systems in different states. The exact place where data are located is not always known and it can change in time. In a public cloud the cloud services are not aimed at specific countries but as ubiquitous services. In this case questions of jurisdiction and applicable law have to be examined.

4.3.2. Applicable law

The contract statute may result from an effective choice of law, from the perspective of European IPL determined by Art. 3 (1) Rome I[31].

In its absence the law of the state applies, where the provider of the service –given that a cloud computing service is qualified as a tenancy law issue– has its «habitual residence», Art. 4 (2) Rome I. If rules of an employment contract shall govern cloud computing, Art. 4 (1b) Rome I leads to the same result.

Furthermore it has to be considered that, for the benefit of consumer protection rules, atypical choice of law clauses are inapplicable; in this case the national law remains applicable, in which the consumer resides, Art. 6 (1b) Rome I. Mandatory national consumer protection rules always remain applicable in favor of the consumer, Art. 6 (2) Rome I.

For companies wanting to store data in the cloud there is a minefield of data protection laws to negotiate, so it is essential to know which country your data is physically stored

30 *Robert Gellman*, «Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing», 23 February 2009, http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

31 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), Official Journal of the European Union, L 177/6 EN

in. «Most organizations don't even know what data they have», says Tony Lock, program director at IT services consultancy Freeform Dynamics. «They are unsure where all the data is and once they've found it they are unsure how to protect it»[32]. But which laws apply, for example, to a German company storing data about German customers via a contract with a US cloud provider whose servers are located in Poland? At the moment –all three– due to the very debatable rules of applicable law in the EU-DPD.

4.3.3. Enforcement

As a consequence the question arises whether the flow of data adequately meet the regulatory requirements of each jurisdiction it flows through. In theory, each controller could be sued in various states worldwide for a breach of data protection laws. But in practice, law enforcement is more difficult.

Data controllers in third countries that want to evade data protection authorities´ oversight can use clouds specifically for that purpose. Another negative effect of the cloud is that any monitoring is contingent on contractual monitoring rights granted by the cloud and resource providers and furthermore these rights must be exercised by the cloud user, which generally has no vested interest in data privacy oversight.

4.4. Contract data processing

If an OES provider receives personal data from the OES user, then the former becomes a data processor[33]. If the processor then outsources this personal data to third parties, giving instructions to further processing of this personal data, a case of sub-processing becomes vital. Between OES user and OES provider practically exists a contract data processing which should include or not include the permission of sub-processing by third parties. As a controller, the cloud user must comply with data protection laws 1) prior to the commencement of the data processing and 2) thereafter through regularly checks that the cloud service provider complies with the technical and organizational security measures. The latter are set out in Art. 17 EU-DPD

Art. 17 (2) EU-DPD imposes on a controller to «implement appropriate technical and organizational controls to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access». Art. 17 EU-DPD remains inapplicable if the processor can be qualified as third entity that does not act on instruction of the controller or the processing of personal data is carried out outside of the E.U. In this case the data transfer is lawful only if the cloud provider complies with the provisions set out in Art. 25 andArt. 26 of the EU-DPD.

---

32 *Juliette Garside*, «How global laws protect your data», The Guardian, 17 October 2011, http://www.guardian.co.uk/cloud-technology/global-laws-protect-your-data

33 see above

Whilst the DPAs acknowledge that it may not always be possible for the cloud user to carry out on-the-spot checks, the cloud user may want to require the cloud service provider to undergo a special certification or seal process. The same obligations essentially apply in relation to sub-processors.

4.5. International data transfer[34]

The EU-DPD states clearly that data cannot leave the EU unless it is transmitted to a country with «adequate level of protection». That means for many cloud providers outside of the EU that they have to study and follow one of four different methods in order to ensure tis adequate protection as long as they wish to conduct cloud services business inside the EU: First, to be one of the countries that have laws enacted that the EU deems to be adequate protection; second, achieve adequacy through compliance with safe harbor provisions; or third, use a standard contractual clause prepared and adopted by the EU; or fourth, use binding corporate rules.

5. FINDING A BALANCE BETWEEN THE CLOUD, ONLINE ENTERTAINMENT AND USERS´ PRIVACY

5.1. Data protection in Germany

At a meeting on 28-29 September 2011[35], the German DPAs with responsibility for the private sector approved a guidance on cloud computing. Although not legally binding, the guidance expresses the view of all German authorities in this field and therefore has de facto relevance for private companies that are subject to German data protection law.

The DPAs impose on cloud providers to improve their design of services in order to comply with German data protection legislation, the Federal Data Protection Act[36]. They also reminded cloud users that they should only make use of cloud services if they are in a position to exercise their obligations as a controller and have checked the implementation of the data protection as well as information security requirements (§ 9 BDSG and its Annex).

In this respect, the German data protection authorities require as a minimum:

- Transparent and detailed information by cloud service providers regarding the technical, organizational and legal framework conditions of the services they offer; transparent, detailed and unambiguous contractual provisions regarding the data processing;

34 This problem has been widely examined by the authors in their contribution to IDP 2011 Conference, «Data transfer from Germany or Spain to third countries – Questions of civil liability for privacy rights infringement», ISBN 978-84-694-7037-4, p. 311 – 340

35 http://www.lfd.m-v.de/dschutz/beschlue/82_DSK/Cloud.pdf

36 Federal Data Protection Act (BDSG), in the version promulgated on 14 January 2003 (Federal Law Gazette I, p. 66), last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I, p. 2814), in force from 1 September 2009

- The implementation of agreed security and data protection measures by both the cloud service provider and the cloud user;
- Up-to-date and meaningful evidence regarding the infrastructure used.

In addition, the German DPAs working groups for technology and media have issued a guidance paper on cloud computing that provides more detail on data protection compliance.[37]

Furthermore, a working group released a paper on data protection issues in OES.[38] The working group noted in particular that the direct integration of social plugins, for example from Facebook, Google + Twitter and other OES on pages of German website owner, without sufficient information to the user and without granting the exercise of consent or not, infringes German and European data protection laws.

Social plugins are just one example of how inadequate some large OES providers handle data protection. For example, Facebook uses face-recognition technology to match displayed images on the Internet to certain people; the affected persons can escape from that only through measures with considerable expenses. Both Facebook and Google+ require that users do have to identify themselves, although under German law, for good reasons, the possibility of at least pseudonymous use of such services must be provided. The data protection officer of the Federal and State Governments are therefore advising to refrain from the use of social plugins which do not comply with data protection standards. The Conference of Data Protection Officers therefore urges the providers of OES to implement decisions that have already been issued in 2008 and 2010 and now repeated in 2011. In this context the DPAs support efforts to develop technical solutions to data protection requirements of web design. Unfortunately, the German federal government did not fulfill its promise of 2011 to announce legislative measures against the profiling on the Internet; it only issued guidance on OES´ voluntary agreements. This could change through the upcoming draft of the Federal Telemedia Act as a step in the right direction.

5.2. Data protection in Spain

There is some criticism[39] on how the EU-DPD was implemented in Spain by the Law 15/99 (LOPD) and its Regulation (ROLPD) set by the Royal Decree 1720/2007. Some of this criticism resulted in the consultation (Case C-468/10) made to the European Court of Justice (ECJ), regarding the Art. 7 (f) of the EU-DPD.

The ECJ clarified that Art. 7 EU-DPD does not allow member states to «introduce principles relating to the lawfulness of the processing of personal data other than those listed in Art. 7 thereof, nor can they amend, by additional requirements, the scope of the six prin-

37 http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

38 http://www.lfd.m-v.de/dschutz/beschlue/82_DSK/Nutzerdaten.pdf

39 *Ana María Marzo Portera*, «Privacidad y Cloud Computing, hacia dónde camina Europa», Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche. V. I número 8. 2012

ciples provided for in Article 7. Attention was called to the fact that the Art. 7 (f) EU-DPD only laid two conditions to the data processing, which were the legitimate interest in the processing and the respect to the fundamental rights of the data subject.

Differently from the EU-DPD, the Art. 10 (1b) RLOPD added a third condition: that data should come from sources available to the public. In view of such addition, the ECJ answered that the second condition brought by the EU-DPD, regarding the processing of data and fundamental rights, should be object of a case-by-case analysis and that the member states were free to set the principles of such analysis, which could include the public source of the information for example. As a consequence, the Spanish Courts decided on 8 February 2012 to declare the nullity of the discussed Art. 10.2 RLOPD. Most recently, the Spanish DPA informed that such decision should be considered[40] as indifferent to the level of data protection in Spain, although there were some different opinions[41].

Another current issue to the Spanish DPA, as other Europeans DPA, was the decision to start paying attention to the OES, especially Facebook. As a consequence, Spain was the only place where it needed to change its minimum age to subscribe, now 14 in Spain and since then both Facebook and AEPD, the Spanish DPA, have frequent conversations in order to achieve a common ground of data protection.

5.3. The European Data Protection Directive and its reform

It is considered that the EU-DPD was not prepared to deal with this variety of issues that the internet would raise concerning privacy[42], not to mention the new internet era of cloud computing. Such urgent call for an updated legal framework was noticed by the E.U. authorities. The European Commission reasoned such need due to the rapid technological development and the increased scale of data sharing[43]. Also, the need of harmonization within the member states motivates the current need of a European Regulation, and not only a review of the EU-DPD. The fact that there was a fragmented implementation of the EU-DPD was reflected in the Resolution of July 6, 2011 of the European Parliament.[44]

Increasing the reach and application of the European legislation, this concept «use of equipment in the EU» from the Art. 4 (1c) of EU-DPD, regarding the territorial scope, is

40 Agencia Española de Protección de Datos. Nota Informativa. El Tribunal de Justicia de la Unión Europea resuelve la cuestión prejudicial planteada por el Tribunal Supremo relative a la Interpretación del artículo 7 f) de la Directiva 95/46/CE

41 Expansión.com, «Las empresas podrán comercializar datos personales sin pedir permiso», http://www.expansion.com/2012/02/13/economia/1329171984.html?a=dc79176f565614fde41d6e17ee32345f&t=1331936892

42 *Bart van der Sloot / Frederik Z. Borgesius*, «Google and Personal Data Protection», Google and the Law Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models, p. 76

43 European Commision. Regulation of the European Parliament and of the Council. 2011

44 European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union

substituted by «(a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behavior».

The definition of consent is also modified, it should now be given in an explicit manner and with the provision of basic information regarding consequences, besides an opt-in system. Such definition will have consequences in e-commerce services, once they will need a statement or a clear affirmative action from the data subject.

In the proposed Regulation, accountability is increased with regard to both data controller (Article 5) and data processor (Articles 26, 31 and 34) as well a more explicit present of the «data minimization» principle. Besides, Art. 6 of the new proposed Regulation states that data processing can only be based on E.U. Law (and not on non-member states), another provision that brings the private data under the European legislative framework.

The need for data controllers based in non-EU member states to appoint a representative based in an E.U. member state (Art. 25) is also present, suggesting spread of the Data Protection Officers (DPOs) in the European Union. The DPOs are common in some member states, such as Germany, where a similar obligation already exists, but it is practically almost inexistent in others, a landscape that will change if this provision is approved.

The complex issue of international data transfer would also be affected by the proposed regulation. It abandons the presumption that no data should be transferred if no adequate level of protection and establishes the conditions under which the data transfer will be permitted. The first one is a declaration of adequacy from the Commission (Art. 41). The second option is the adoption of appropriate safeguards such as binding corporate rules, data protection clauses and standard clauses (Art. 42). The last possibility is to make use of a modified EU-DPD derogation, in the proposed Art. 44 it is requested that more information is provided to the data subject.

As a whole, the proposed regulation clearly foresees the need of an efficient, effective and harmonized legislation for data protection in the E.U. The technological developments and the large scale of data transfer since the EU-DPD are taken into consideration. The result is a proposal that might take data protection in the E.U. to a higher level, for data controllers, -processors and last but not least the -subject.

5.4. International framework for data protection

To come to the point. There is yet no international and binding legal framework in place to regulate privacy and data protection issues[45], especially in a cloud computing environment. Even among E.U. member states there are some relevant implementation differences. Like expected, global harmonization is very difficult to reach and member states try to call for its own jurisdiction, bringing processed data literally «homewards», either European, American or other.

45 *Philipp Fischer*, Will Privacy Law in the 21st Century be American, European or International?

6. FUTURE SOLUTIONS TO EXISTING PROBLEMS

According to Peter Hustinx[46], European Data Protection Supervisor, there is a current «hunger» for more and more data. Three main actions should be taken in order to avoid that that hunger affects data protection: 1) Improve existing solutions of the law (6.1.), supported by 2) technical solutions (6.2.) and 3) guidelines of the private sector, DPAs and policy makers (6.3.).

These three «musketeers», one for all, all for one - could be a future solution:

6.1. Solutions of the law

Legislative solutions are not an exclusivity of the E.U.. Uruguay, Argentina and New Zealand for example, approved legislations on data protection that were considered to be satisfactory. The issue at stake might not be the lack of solutions, but the concretizations of the solutions in a legislation that imposes duties to the companies processing and controlling personal data. Existing national, regional and international legal frameworks to be examined are:

6.1.1. U.S.

A Self-certification program of U.S. companies to safe harbor is not enough to reach a data security level corresponding to E.U. standards. Also cloud contracts which are orientated by safe harbor are insufficient. Safe harbor cannot however serve to handle the stricter data security regulations in Europe. Coud suppliers like Google or Salesforce with headquarter in the U.S. identify themselves for the purpose of proof of her trustworthiness with a SAS-70-Typ-II certificate. This means that the data centres should be checked by independent third. This measure is enough only partially for the requirements of the order data processing. It does not consider, e.g., the material and procedural interests of affected person's in transmissions. It is also possible that the companies involved in a Cloud present themselves to BCRs, by which an adequate level of protection after Art. 26 par. 2 EU-DPD could be reached.

6.1.2. E.U.

Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda EU Data protection reform and Cloud Computing, tried to sum positive impacts of the data protection reform for cloud businesses saying that proposed rules should make it easier to operate in clouds cross borders, beneficing global businesses for example seeking permission from one single authority[47]. In the authors' opinion there are still some issues that have to be addressed in the reform´s further consultations:

---

46 *Peter Hustinx*; «Building Privacy for the Future». Speech at the Future Internet Assembly, Ghent, 16 December 2010.

47 *Neelie Kroes*, Vice-President of the European Commission responsible for the Digital Agenda EU Data protection reform and Cloud Computing «Fuelling the European Economy» event, Microsoft

- The future concept of personal data in the cloud should be based on the realistic risk of identification. Whether data protection rules apply or not should be based on all facts of the situation which carry the risk of harm. It should also be clarified which procedures for encryption or anonymization are accepted in future legislation.
- The current legal uncertainties exist because data protection laws may differ between EU member states and that practical recommendations are needed relating to whether the Directive can be enforced in non-EU countries. Therefore, clarification is needed by the Commission on which and when country's security requirements and other rules do apply to a cloud computing user or provider. The European framework on data protection is still based on the country of origin rule, and the proposed Regulation on the residence of the data subject. Both criteria seem insufficient to bring clarity and legal certainty in data protection.
- The Directive fails to acknowledge the interacting positions between controller and processor in a cloud surrounding. They may overlap and cloud computing service providers be unaware that the data they process or store on behalf of a customer is classified as 'personal data', possibly because the controller lacks to inform the processor. Ian Walden, Professor of Information and Communications Law, says: «There should be different levels of responsibility depending on the nature of the service being provided.»[48]
- When the case of data being exported out of the E.U, the restriction should be according to «accountability, transparency and security. It is not where information is stored, but how securely it is stored, and who can access it, that matters most,»[49] says Kuan Hon, paper co-author and researcher on the Cloud Legal Project[50]. Until then, there must have compliance with a plurality of national regulations whilst should make use of data security certifications and independent third party audits.

6.1.3. Bilateral conventions

At the same time of European Commissions consultations on the reform, a new bilateral E.U.-U.S. agreement could be drafted, being a first important step in bridging the existing differences on the application of data protection laws, «it would make it then easier to achieve a common approach on protecting personal data online in the businesses world»[51].

Executive Briefing Centre Brussels, 30 January 2012, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/40&format=HTML&aged=0&language=EN&guiLanguage=en

48 *Ian Walden / Christopher Millard / Kuan Hon*, «Data protection law creates cloud of uncertainty for cloud computing», 21 November 2011, http://www.ccls.qmul.ac.uk/news/2011/59982.html

49 *Ian Walden / Christopher Millard / Kuan Hon*, «Data protection law creates cloud of uncertainty for cloud computing», 21 November 2011, http://www.ccls.qmul.ac.uk/news/2011/59982.html

50 http://www.cloudlegal.ccls.qmul.ac.uk/

51 *Viviane Reding*, «Privacy standards in the digital economy: enhancing trust and legal certainty in transatlantic relations», 23 March 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/210

Although the E.U. is negotiating with the U.S. on data protection in judicial and police cooperation in criminal matters, it will not constitute in itself the legal basis for transfers of personal data related to cloud computing issues. Such transfer of personal data will still require a specific agreement providing a legal basis. An E.U.-U.S. agreement could become the reference for data protection standards that apply whenever personal data needs to be transferred across the Atlantic.

6.1.4. Multilateral conventions

A multilateral convention could produce a greater degree of harmonization, since it results in a single text that is legally binding on states that enact it. But such binding nature can also make states reluctant to do so. The possible convention could be faced with reservations made by States that are party to it, which can result in a diminution of the very harmonisation that the convention was supposed to accomplish, and a convention can be difficult to amend in the face of changing practices or technological evolution[52]. The problem of a lack of forum that could hold such discussion is also a barrier, once the existing organizations are mostly too specialized and may not be well-prepared to produce standards in an area as diverse and multi-faceted as privacy. Last but not least the Asia-pacific economic cooperation (APEC) framework could be designed to be a more flexible system than the E.U. adequacy approach. It could be implemented in the vastly differing cultural and legal frameworks of the APEC Member States.

6.2. Technical solutions

6.2.1. Self-certification and international standards

Elements of self-control in fact do support compliance with data protection laws only if each partner of the cloud service contract meets the guidelines´ requirements. The problem remains for cloud users how to prove that the contract partner fulfills all requirements set out in the contract. Approaches could be:

- conclusion of a Service Level Agreement (SLA)
- periodical control / audit (not realizable in a dynamic cloud surrounding)
- ISO 27000
- BSI (cloud user within Germany) or ENISA (cloud user within E.U.) guidelines
- agree upon a Privacy Seal, e.g. the Privacy Seal of the Data Protection Authority of Schleswig-Holstein[53]

52 *Souichirou Kozuka*, «The economic implications of uniformity in law», in: Uniform Law Review, 2007, part 4, p. 683-696, http://www.unidroit.org/English/publications/review/articles/2007-4-kozuka-e.pdf, p.693, stating that «ironically, the more popular a Convention is, the more difficult it is to amend the uniform law in a timely manner«

53 https://www.datenschutzzentrum.de/faq/guetesiegel_engl.htm

- common criteria
- restriction on networks of trusted partners instead of direct audits

ISO, the International Organization for Standardization, developed international standards in many areas that are essential to everyday life. On technology standards ISO and IEC, the International Electrotechnical Commission, which is responsible for standards in the field of electrics and electronics, are cooperating together. Through a privacy-friendly design of these standards at an early stage, potential risks for privacy of individuals could be reduced or entirely eliminated. Unfortunately, the Data Protection Authorities do rarely have an adequate possibility, due to their existing equipment and staff and the great variety of technical standards, to apply their expertise in the relevant bodies.

The «Privacy Toolkit»[54], published by the Task Force on privacy and the protection of personal data of the International Chamber of Commerce (ICC), is an example for another private sector instrument. This toolkit is an international business guide for policymakers and aims at governments seeking an innovative approach to privacy that balances the needs of governments, individuals and the economy as a whole. It outlines guiding principles for privacy that draw upon the OECD privacy guidelines, and suggests practical ways to put the principles to work.

6.2.2. Privacy by design principles

a) EU data protection reform and PbD principles

Privacy by Design is a concept brought to light by Ann Cavoukian, Information & Privacy Commissioner Ontario, Canada.

The EU data protection reform foresees the application of these principles. Thus, this paragraph will try to draw a line between PbD in present practice and its possible future implications under the E.U. Commission´s draft.

b) Short Analysis of the 7 PbD principles

- Proactive not Reactive; Preventative not Remedial

«The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred - it aims to prevent them.»[55]

Appropiate proactive measures in order to guarantee an adequate level of data protection can never provide a 100% protection. Guidelines and processes provided by EU-DPD and BDSG will still be necessary. Ann Cavoukian asks in her «Fair Information Principles«

54 http://www.iccwbo.org/uploadedFiles/TOOLKIT.pdf

55 http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

controllers to accept self-certify for data protection levels even higher than in current legal provisions; an unreachable aim.

- Privacy as the Default Setting

«We can all be certain of one thing –the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy– it is built into the system, by default.»[56]

The idea of privacy by default already does exist under German law. The reform of the BDSG changed the default setting from «opt-out» to «opt-in», meaning that since then, every owner of personal data has to explicitly express its consent before a processing of its personal data. The «Payback» and «Happy Digits» decisions of the German Federal Court (BGH) underlined, that opt-in must be the default and opt-out the exception. The proposed EU-DPD includes that principle as well («Whenever consent is required for data processing, it will have to be given explicitly, rather than be assumed»)

- Privacy Embedded into Design

«Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.«[57]

It is clear that only if privacy requirements are defined early, the protection of personal data can be taken into account in the design phase. Today, in many cases, data protection is too late implemented or tested. E.g. in a product lifecycle of software , whole database structures, views, user interfaces and concepts could be defined that way that data protection provisions are met at all levels (data storage, logic and GUI). In practice, because too costly, this has rarely been the case.

- Full Functionality – Positive-Sum, not Zero-Sum

«Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum «win-win» manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.»[58]

Privacy by design requires that functionality, security and privacy are not in conflict, leading to a «win-win» situation. To resolve potential conflicts all requirements three have to be identified from the beginning. The new EU-DPD would «give you more control over your personal data, make it easier to access, and improve the quality of information you get about what happens to your data once you decide to share it. These proposals are designed

56 http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

57 http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

58 http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

to make sure that your personal information is protected –no matter where it is sent or stored– even outside the EU, as may often be the case on the Internet.» People having more control over the way their data will be processed will certainly have a negative impact on functionality.

- End-to-End Security – Full Lifecycle Protection

«Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.»[59]

The principle of end-to-end security refers to the life cycle of personal data. It should be dealt with personal data in a lawful way from the beginning of its collection, over its process until its use. According to Article 15 paragraph 2 of the EU Commission´s draft, companies that have deleted data subject´s content on their request, also have to make sure that any links or copies of the deleted information are from now on available to the public. The requirement to protect data in its complete life cycle, can, at least implicitly, deduced from § 9 BDSG and its annex (technical and organizational measures) which of course refers to personal data in all «stages of life», otherwise the BDSG would suffer an unsystematic and dangerous gap in law.

In practice however it may be difficult to find the controller or processor who is responsible for the data. In addition, there are numerous data collections the data subject is not even aware of. Especially in cloud computing surroundings the distinction between controller and processor is not always clear in practice and has to be subjected to a comprehensive consideration of all circumstances, especially if a cloud service is offered on a cross-border basis or cloud sub-providers are included in the supply chain. At this point the focus has to –again– lie on the concept of «data controller» and «data processor», of the EU-DPD.

- Visibility and Transparency – Keep it Open

«Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.«[60]

The data subject should know no restrictions on how and where their data is stored, processed or analyzed, a complete traceability of the process is required and should be checked regularly, because trust is good, control is better. This includes for each data subject the opportunity to lodge a complaint or requested access to data. These rights are also required by the BDSG, although implementation in practice has not always run smoothly. From a German

59 http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

60 http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

Data Protection Officers point of view it can be stated that data breach notifications are likely to be far from being completely published and communicated to data subjects. While the EU commissions draft foresees notification of interested parties within 24 hours, the BDSG speaks of an «immediate» notification time without specific indication. In addition, many international companies such as Facebook or Google are subjected to European and German law only on a limited basis. First steps towards more transparency have been made for example made through the audit of Facebook by the Irish Data Protection Authority, although the results remain controversial. Nevertheless, tests of international companies based in Europe continue to be driven by the regulatory authorities. This could lead to an early detection of bad apples and increase awareness for internal or external data protection audits.

- Respect for User Privacy – Keep it User-Centric

«Above all, PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.«[61]

Adequate data protection rules should be guided primarily by the interests of individuals, each data subject should be able choose to adjust their privacy settings through extensive configuration determining what information they want to disclose about themselves for whom and for what purposes they are used. Even an anonymous use would be conceivable if there is no legal need for the real name, e.g. for given business purposes . This user-oriented approach exists in the BDSG.

6.3. Solutions of the private sector

A common base could be reached between private sector, DPAs and policy makers especially regarding the users consent and the possibility of the user to comply with laws set out to regulate a data controllers´ obligations. Terms of use could provide an adequate protection of personal data if some key issues have been observed in the contractual relationship between cloud provider and cloud user:

- Anonymization of the data for transborder data flow is possible
- Movement of data will be controlled
- Data encryption is provided
- Cloud user can access all of data anytime anywhere
- Exit scenarios for the future transfer of the data to other cloud providers
- Backup/restore plan
- Data breach notification
- Service levels and emergency plan in case of unavailability
- Commitment can be obtained regarding
  – the place where the data will be processed

61 http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

– the exact supply chain
– contract parties, their roles, rights and obligations, especially in case of multiple cloud platforms involved
– the period of data retention and treatment of data after termination or insolvency

7. CONCLUSION

Along with new cloud computing services, OES and pervasive privacy, the concept of reasonable expectation of privacy is, in fact, becoming an expectation of being monitored. Notwithstanding, users are not aware of the number of processes running in the background and most important, which data those processes gather, for which purposes and with who is it shared with.

As a response, countries are considering to adopt stronger legislation on data protection. The brainstorming of solutions, sometimes as a feedback to implementation of pervasive computing, resulted in the proposals for the adoption of technical features. One of the most celebrated technical solution is the PbD, seen by policy makers as an urgent need.

On the other side, industry and part of stakeholders are of the opinion that legislations imposing burdensome procedures, obligations, and restrictions regarding data protection might slow down the current development path and mine the benefits of ICT for end users and in certain countries.

These three main stakeholders: users, ICT companies and policy makers have been struggling to find a satisfactory solution to all-parts. This is the current challenge for both the European Union, United States and countries in general, all of them having its citizens' privacy affected by new technologies.

8. BIBLIOGRAPHY

Books and monographs

Fischer, P. (2012). Will Privacy Law in the 21st Century be American, European or International? Munich: GRIN Verlag.

Lessig, L. (2006). Code version 2.0. New York: Basic Books.

Electronic documents

Agencia Española de Protección de Datos (2011). Nota Informativa. El Tribunal de Justicia de la Unión Europea resuelve la cuestión prejudicial planteada por el Tribunal Supremo relative a la Interpretación del artículo 7 f) de la Directiva 95/46/CE. 24 November 2011. https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2011/notas_prensa/common/noviembre/111124_sentencia_TJUE.pdf

Article 29 Data Protection Working Party (2007). Opinion 4/2007 on the concept of personal data. 20 June 2007. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Article 29 Data Protection Working Party (2009). Opinion 5/2009 on online social networking. 12 June 2009. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf

Article 29 Data Protection Working Party (2009). The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. WP 168. 1 December 2009. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

Article 29 Data Protection Working Party (2010). Opinion 1/2010 on the concepts of «controller» and «processor». 16 February 2010. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

Article 29 Data Protection Working Party (2010). Opinion 3/2010 on the principle of accountability 1- 19. Retrieved March 13, 2012 from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

Article 29 Data Protection Working Party (2011). Opinion 16/2011 on EASA/IAB Best Practice Recommendation Advertising. 1- 13. Retrieved March 13, 2012 from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf

Article 29 Data Protection Working Party (2012). Letter to OBA Industry, IAB Europe and EASA. 1 March 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120301_reply_to_iab_easa_en.pdf

Cavoukian, A. (2011). Privacy by Design. The 7 Foundational Principles. January 2011. http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

Council of European Professional Information Societies (CEPIS). (2008). Social Networks – Problems of Security and Data Privacy. Background Paper. Retrieved on February 20, 2012 from http://www.cepis.org/files/cepis/20090901104125_CEPIS%20social%20network%20Backgroun.pdf

Council of European Professional Information Societies (CEPIS). (2008). Social Networks – Problems of Security and Data Privacy. Statement. Retrieved on February 20, 2012 from http://www.cepis.org/files/cepis/20090901104132_CEPIS%20social%20network%20statement.pdf

de Hert, P. / Schreuders, E. (2001). The Relevance of Convention 108. European Conference on Data Protection on Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data: present and future. Data Protection Conference (2001) Reports, p. 63-76, The Council of Europe (ed.), http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/events/conferences/DP%282001%29Proceedings_Warsaw_EN.pdf

Efrati, A. (2011) 'Like' Button Follows Web Users. 18 May 2011. http://professional.wsj.com/article/SB10001424052748704281504576329441432995616.html?mod=rss_Technology&mg=reno-secaucus-wsj

European Commission (2012). How does the data protection reform strengthen citizens' rights? http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf

European Commission (2012). Why do we need an EU data protection reform? http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf

G8 Declaration (2011). Renewed committment für freedom and democracy. G8 Summit of Deauville. 26-27 March 2011. http://www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html

Garside, J. (2011). How global laws protect your data. The Guardian. 17 October 2011. http://www.guardian.co.uk/cloud-technology/global-laws-protect-your-data

Gellman, R. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. 23 February 2009. http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

Hogge, B. (2010). Open Data Study. Commissioned by the Transparency and Accountability Initiative. Retrieved January, 9th, 2012 from http://www.soros.org/initiatives/information/focus/communication/articles_publications/publications/open-data-study-20100519/open-data-study-100519.pdf

Hustinx, P. (2010). Building Privacy for the Future. Speech at the Future Internet Assembly, Ghent, 16 December 2010. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-16_future_internet_assembly_EN.pdf

International Chamber Of Commerce (2003). Privacy toolkit. An international business guide for policymakers. November 2003. http://www.iccwbo.org/uploadedFiles/TOOLKIT.pdf

Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2011). Arbeitskreise Technik und Medien. Orientierungshilfe – Cloud Computing. 26 September 2011. http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2011). Datenschutz bei sozialen Netzwerken jetzt verwirklichen! 28./29. September 2011. http://www.lfd.m-v.de/dschutz/beschlue/82_DSK/Nutzerdaten.pdf

Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2011). Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing. 28./29. September 2011. http://www.lfd.m-v.de/dschutz/beschlue/82_DSK/Cloud.pdf

Konjovi, G. (2010). Wieso wir den Facebook «Like-Button» wieder entfernten. 22 June 2010. http://intern.hamburg.de/2010/06/22/wieso-wir-den-facebook-like-button-wieder-entfernten

Kroes, N. (2012). EU Data protection reform and Cloud Computing. 30 January 2012. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/40&format=HTML&aged=0&language=EN&guiLanguage=en

Kuner, C. (2012) The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. Retrieved on February 10, 2012 from http://www.hunton.com/files/Publication/9818f6ae-7cca-401b-920f-961dffa18ea2/Presentation/PublicationAttachment/5df1365f-d659-4c06-96e5-984a4cfeffd6/Kuner_EU_regulation_020612.pdf

Kye, C. I. / Stern G. (2011). Where in the World is My Data? Jurisdictional Issues with Cloud Computing. 30 March 2011. http://www.fasken.com/files/Event/3195cb2b-f29b-456d-8f98-7a3175930523/Presentation/EventAttachment/aea8833f-ab3c-48f1-854d-6ec4be989775/Jurisdictional_Issues_with_Cloud_Computing_Ian_Kyer_Gabriel_Stern.pdf

Marín López, J. J. (2012) El tratamiento de datos personales sin consentimiento del intresado tras la sentencia del Tribunal Supremo, Sala 3, de 8 de febrero de 2012. Retrieved on March 20, 2012 from http://www.uclm.es/centro/cesco/pdf/trabajos/28/2012/28-2012-1.pdf

Martinez, D. (2010). Cloud Computing: El derecho y la política suben a la nube. 1- 25 Retrieved from March 20, 2012 from http://idp.uoc.edu

Microsoft. (2010) Privacy in the Cloud Computing Era. Retrieved on March 12, 2012 from http://go.microsoft.com/?linkid=9694913

Microsoft. (2010). The Economics of the Cloud. Retrieved on February 10, 2012 from http://www.microsoft.com/presspass/presskits/cloud/docs/The-Economics-of-the-Cloud.pdf

Miralles, Ramón (2010) Cloud Computing y protección de datos. Retrieved on January 25, 2012 from http://idp.uoc.edu

NEC Co. Ltd. Inf. And Privacy Commissioner, Canada (2010)Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach Retrieved on March 13, 2012 from www.privacybydesign.ca

Portera, A. M. M. (2011) Privacidad y Cloud Computing, Hacia Dónde Camina Europa. Retrieved on March 17, 2012 from http://revistasocialesyjuridicas.files.wordpress.com/2012/02/08-tm-12.pdf

Puente Escobar, A. (2011). Informes y Sentencias Relevantes. 4ª Sesión Anual Abierta de la AEPD. https://www.agpd.es/portalwebAGPD/jornadas/4_sesion_abierta_2011/common/Consultas_iinformes_sentencias_relevantes.pdf

Reding, V. (2010). Privacy matters – Why the EU needs new personal data protection rules. 30 November 2010. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700

Reding, V. (2011) Privacy standards in the digital economy: enhancing trust and legal certainty in transatlantic relations. 23 March 2011. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/210

Renub Research. (2010). Cloud Computing – SaaS, PaaS, IaaS Market, Mobile Cloud Computing, M&A, Investments, and Future Forecast, Worldwide. Retrieved from March 2, 2012 from http://renub.com/reports/showdetails.aspx?id=30

Research Centre on IT and Law (CRID). (2010). Cloud Computing and its implication on data protection. 1- 30. Retrieved from March 2, 2012 from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1b.pdf

Rossbach, C. Welz, B. (2011). Survival of the fittest. How Europe can assume a leading role in the cloud. Retrieved March 13, 2012 from http://www.rolandberger.com/media/publications/2011-11-22-rbsc-pub-Survival_of_the_fittest.html

Schiering, I. / Hansen, M. (2010).Sind Privacy und Compliance im Cloud Computing möglich? 4 March 2010. https://www.datenschutzzentrum.de/vortraege/20100304-cebit-heise-schiering-hansen-cloud-computing-datenschutz-privacy.pdf

Serraller, M. (2012). Las empresas podrán comercializar datos personales sin pedir permiso. 13 February 2012. http://www.expansion.com/2012/02/13/economia/1329171984.html?a=dc79176f565614fde41d6e17ee32345f&t=1331936892

Smith, D. M. (2011). Key Issues for Cloud Computing. 1- 9. Retrieved March 13, 2012 from http://cloud.ctrls.in/files/key-issues-for-cloud-computing.pdf

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) (2011). Dialog with Facebook does not hinder data protection enforcement. 30 September 2011. https://www.datenschutzzentrum.de/presse/20110930-facebook-enforce-privacy.html

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) (2011). ULD an Webseitenbetreiber: «Facebook-Reichweitenanalyse abschalten«. 19 August 2011. https://www.datenschutzzentrum.de/presse/20110819-facebook.htm

Walden, I. / Millard, C. / Hon, K. (2011). Data protection law creates cloud of uncertainty for cloud computing. 21 November 2011. http://www.ccls.qmul.ac.uk/news/2011/59982.html

Zynga Corp. (2011). Privacy Policy. 30 September 2011. http://company.zynga.com/about/privacy-center/privacy-policy

Book Chapters

Fischer, P. / Ferraz Vazquez, R. (2011). Data transfer from Germany or Spain to third countries – Questions of civil liability for privacy rights infringement. In: Cerrillo, A., Peguera, M., Peña, I., Vilasau, M. (ed.). Net Neutrality and other challenges for the future of the Internet. Proceedings of the 7th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya, Barcelona, 11-12 July. 311-340

García Macho, R. (2010). El derecho a la información, la publicidad y la transparencia en las relaciones entre la administración, el ciudadano y el público. In Ricardo García Macho (ed.), Derecho administrativo de la información y administración transparente (pp. 27-47). Madrid: Marcial Pons.

Van der Sloot, B., Borgesius, F. (2011). Google and Personal Data Protection. In: Aurelio Lopez-Tarruela (ed.), Google and the Law – Empirical approaches knowledge-economy business models (1st ed., pp 403). The Hague: Springer.

Journal Articles

Clarke, R. (2011). An evaluation of privacy impact assessment guidance documents. International Data Privacy Law, 1(2), 111- 119.

Dubois, P., (2011). EU Applicable law: clarification on some practical issues relating to data protection – from Article 29 29 Working Party´s Opinion 8/2010. Computer and Telecommunications Law Review, 17(4), 97- 136.

Fuchs, C. (2011). An alternative view of privacy on Facebook. Information, 2, 140- 165.

Grant, H. (2009).Data protection 1998-2008. Computer Law & Security Review, 2009, vol. 25, iss. 1, 44-50

Greenleaf, G. (2009). Five years of the APEC privacy Framework: Failure or promise?. In: Computer Law & Security Review, 2009, vol. 25, iss. 1, 28-43

Greer, D. (2011). Safe Harbor – A framework that works. International Data Privacy Law, 1(3), 143- 148.

Hon, W. K., Millard, C., Walden, I. (2011). The problem of personal data in the cloud computing: what information is regulated – the cloud of unknowing. International Data Privacy Law, 1(4), 211- 220.

Hon, W. K., Millard, C., Walden, I. (2011). The problem of personal data in the cloud computing: what information is regulated – the cloud of unknowing. Part 2. International Data Privacy Law, 2(1), 3- 12.

Kozuka, S. (2007). The economic implications of uniformity in law. In: Uniform Law Review, 2007, part 4, 683-696

Kuner, C. (2009). An international legal framework for data protection: Issues and prospects. Computer Law & Security Review, 2009, Vol. 25, 307-317

Kuner, C. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. OECD Digital Economy Papers No 187, 1- 32.

Marzo Portera, A. M. (2012). Privacidad y Cloud Computing, hacia dónde camina Europa. Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche. V. I número 8. 2012

Moerel, L. (2011). Back to basics: When does EU data protection law apply? International Data Privacy Law, 1(2), 92- 101.

Ponce, J. (2002). Good Administration and European Public Law. European Review of Public Law, 14(4), 1503-1544.

Warren, S. / Brandeis, L. (1890). The Right to Privacy. Harvard Law Review, Vol. IV No. 5, 15 December 1890.

Wotjan, B. (2011). The new EU Model Clauses: One step forward, two steps back? International Data Privacy Law, 1(1), 76- 80.

EL RETO DE LA PROTECCIÓN DE DATOS DE LAS PERSONAS MAYORES EN LA SOCIEDAD DEL OCIO DIGITAL

Isidro Gómez-Juárez Sidera
Doctorando en la Universitat Politècnica de València.
Facultad de Administración y Dirección de Empresas

María de Miguel Molina
Profesora Titular de la Universitat Politècnica de València.
Departamento de Organización de Empresas

RESUMEN: Internet tiene en la actualidad un amplio campo de negocio en el ámbito de las personas mayores. Según previsiones de las Naciones Unidas, para el año 2050 el número de personas mayores de 60 años casi se triplicará, generándose oportunidades en el mercado de bienes y servicios que responda a sus necesidades. En este sentido, el mundo digital ofrece, bajo una falsa apariencia de gratuidad, una infinidad de servicios de ocio y entretenimiento en los que la contraprestación es nuestra propia información personal. En dicho escenario, las personas mayores constituyen uno de los eslabones más débiles de la sociedad digital por efecto de la denominada «brecha generacional digital» y el progresivo deterioro físico, sensorial, mental y cognitivo que convierte a los mayores en un colectivo social de riesgo por su especial fragilidad. Para superar con éxito el reto de la protección de datos de las personas mayores en la sociedad del ocio digital, es necesaria una estrategia pluridimensional y omnicomprensiva de la problemática de este colectivo de especial sensibilidad, basada en una serie de puntos clave que se exponen en el presente trabajo con el objetivo de servir de base tanto en el ámbito académico como profesional, así como a las empresas que ofrezcan estos servicios y cuenten entre su público objetivo a los mayores.

PALABRAS CLAVE: personas mayores, protección de datos, sociedad digital, ocio digital, entretenimiento online.

1. LAS PERSONAS MAYORES EN LA SOCIEDAD DEL OCIO DIGITAL

1.1. Las personas mayores en la sociedad digital

El Plan de Acción Internacional sobre el Envejecimiento (1982)[1] fue el primer instrumento orientado a la creación y aplicación, en los planos internacional, regional y nacional, de políticas destinadas a mejorar la vida de los ancianos como individuos y a mitigar, con medidas apropiadas, cualquier efecto negativo resultante de la repercusión del envejecimiento de las poblaciones en el desarrollo.

1 Aprobado en la primera Asamblea Mundial sobre el Envejecimiento, celebrada en Viena, Austria, del 26 de julio al 6 de agosto de 1982, y que la Asamblea General de las Naciones Unidas hizo suyo en su Resolución «37/51. Cuestión del envejecimiento», de fecha 3 de diciembre de 1982.

Unos años más tarde, la Federación Internacional de la Vejez (FIV)[2], entidad privada sin ánimo de lucro, decide redactar una «Declaración de Derechos y Responsabilidades de las Personas de Edad», con la finalidad de que ésta fuese recogida y aprobada por la Organización de las Naciones Unidas. La citada declaración se basaba en la Declaración Universal de Derechos Humanos aprobada por las Naciones Unidas en 1948, así como en muchas otras declaraciones adoptadas por las Naciones Unidas a través de los años, como las que se relacionaban con la mujer, el niño, el retraso mental, etc., y tenía por objeto complementar la Declaración Universal, no reemplazarla, y tratar de destacar las consecuencias de la Declaración Universal en lo que se refería a las personas de edad. Asimismo, incorporaba varios principios del propio Plan de Acción Internacional sobre el Envejecimiento sobre los que ya existía un cierto consenso internacional.

Sobre la base de los cimientos asentados en la Carta de las Naciones Unidas, la «Declaración de Derechos y Responsabilidades de las Personas de Edad» de la Federación Internacional de la Vejez y el reconocimiento de las aportaciones que las personas de edad hacían a sus respectivas sociedades, la Asamblea General de las Naciones Unidas, convencida de que es menester proporcionar a las personas de edad que deseen y puedan hacerlo posibilidades de aportar su participación y su contribución a las actividades que despliega la sociedad, estableció en 1991 una serie de normas universales para las personas de edad en cinco ámbitos principales: independencia, participación, atención, realización personal y dignidad. Aprobados en su Resolución 46/91, de fecha 16 de diciembre de 1991, los «Principios de las Naciones Unidas en favor de las personas de edad» recogen, entre otros, que «Las personas de edad deberán permanecer integradas en la sociedad…» (Principio 7) y «… poder aprovechar las oportunidades para desarrollar plenamente su potencial…» (Principio 15).

Ahora bien, para su plena integración en nuestra sociedad actual como sujetos activos, las personas mayores deben enfrentarse, de manera insoslayable, al reto de las nuevas tecnologías. No en vano, el objetivo marcado por las Naciones Unidas en la Estrategia Internacional de Acción sobre el Envejecimiento 2002 es el de garantizar que las personas de todos los lugares puedan envejecer con seguridad y dignidad y continuar participando en sus sociedades como ciudadanos de pleno derecho, en particular mediante el uso de las nuevas tecnologías.

En opinión de Ji et al.[3], en las dos últimas décadas hemos sido capaces de gestionar nuestra sociedad sin tener en cuenta, hasta cierto punto, las necesidades específicas de las personas mayores en el contexto digital. No obstante, la proporción de personas mayores aumenta de forma vertiginosa: de acuerdo con las previsiones de las Naciones Unidas, para el año 2050 el número de personas mayores de 60 años casi se triplicará, pasando de 737 millones en 2009 a 2.000 millones. Ello obliga a replantear determinadas estrategias si queremos aspirar a una sociedad digital incluyente cuyos beneficios estén al alcance de todos.

---

2 International Federation on Ageing, IFA.

3 Ji, Y. G. et al. (2010). Older Adults in an Aging Society and Social Computing: A Research Agenda. *International Journal of Human-Computer Interaction, 26 (11-12)*, 1122-1146. doi: 10.1080/10447318.2010.516728

1.2. Personas mayores y ocio digital

Siguiendo a Nimrod[4], mantenerse comprometido con la vida de manera activa es un aspecto clave para un envejecimiento exitoso. En este sentido, las actividades de ocio pueden proporcionar a las personas mayores los medios necesarios para permanecer física, social y mentalmente activas y exteriorizar sus fuerzas e intereses frente a las limitaciones propias de la edad.

La doctrina distingue entre el ocio serio y el ocio casual. El ocio serio se caracteriza por el compromiso, esfuerzo y perseverancia y se asocia con muchas recompensas psicológicas duraderas (vgr. actividades de voluntariado, participar en un grupo de teatro aficionado, etc.). Por el contrario, el ocio casual se define como «una actividad inmediata, intrínsecamente gratificante, con un núcleo placentero relativamente momentáneo, que requiere poca formación (o no especializada) para disfrutar de ella»[5].

En relación al impacto de las nuevas tecnologías sobre las personas mayores, debemos distinguir entre aquellas tecnologías dirigidas a la tercera edad o mayores jóvenes (entre 65 y 80 años), enfocadas a favorecer su inclusión y participación en la sociedad y mejorar su calidad de vida, y las tecnologías destinadas a la cuarta edad o mayores frágiles (más de 80 años), pensadas para personas con un mayor deterioro físico y mental, cuyo principal propósito es proporcionarles unos niveles superiores de seguridad y autonomía personal. Internet se ubica dentro del primero de ambos grupos, ofreciendo nuevas formas de ocio casual a las personas mayores: Nimrod[6] cita, entre otros, los juegos en línea, pasatiempos virtuales, álbumes de fotos digitales y, por supuesto, las redes sociales.

De tal manera, las redes sociales han dejado de ser coto vedado de jóvenes y adolescentes, perfilándose como la «medicina del futuro» para curar la soledad de la vejez a través de un medio en el cual mantenerse socialmente activo y compartir sentimientos, experiencias y recuerdos. En este sentido, Nimrod[7] señala que la práctica del sentido del humor en las comunidades en línea, así como la oportunidad que ofrecen a las personas mayores de demostrar sus capacidades y habilidades sociales y disfrutar del reconocimiento de los demás, hacen de éstas un medio importante para hacer frente al envejecimiento. Asimismo, la participación en la cultura del entretenimiento digital a través de las comunidades en línea contribuye a la integración y compromiso social de las personas mayores, incluso cuando sus redes sociales *offline* se hayan restringido como consecuencia del deterioro físico y las muertes de sus amigos. Finalmente, si bien la participación de las personas mayores en la

4 Nimrod, G. (2011). The Fun Culture in Seniors' Online Communities. *The Gerontologist*, *51 (2)*, 226-237. doi: 10.1093/geront/gnq084

5 Stebbins, R. A. (1997). Casual leisure: A conceptual statement. *Leisure Studies*, *16*, 17-25. doi: 10.1080/026143697375485

6 Nimrod, G. (2010). Seniors' online communities: A quantitative content analysis. *The Gerontologist*, *50*, 382-392. doi:10.1093/geront/gnp141

7 Nimrod, G. (2011). The Fun Culture in Seniors' Online Communities. *The Gerontologist*, *51 (2)*, 226-237. doi: 10.1093/geront/gnq084

cultura del entretenimiento digital no tiene ninguna contribución demostrable en la mejora de su salud física, ésta ofrece alternativas de ocio agradable y variado que pueden sustituir y, en cierta medida, compensar la pérdida de oportunidades de participar en actividades al aire libre a aquellas personas mayores que sufran problemas de movilidad.

1.3. Estrategias para afrontar el reto de la protección de datos de las personas mayores

Carpenter y Buday[8] apuntan con acierto que, al margen de la complejidad de su uso, una de las principales razones de la escasa utilización de las nuevas tecnologías por los usuarios de más edad estriba en los problemas relativos a la seguridad y la protección de la privacidad. No en vano, el mundo digital ofrece, bajo una falsa apariencia de gratuidad, una infinidad de servicios de ocio y entretenimiento en los que la contraprestación es nuestra propia información personal. En este escenario, las personas mayores constituyen uno de los eslabones más débiles de la sociedad digital. Por tanto, si bien las tecnologías de la información y la comunicación (TICs) pueden proporcionar oportunidades a los mayores, también pueden suponer ciertas amenazas. En un plano más específico, sucede asimismo con las actividades de ocio online (Tabla 1).

Al igual que sucede con otros grupos, como por ejemplo los menores de edad[9], la persona mayor puede simplemente utilizar lo que le brinda la Red (receptora de contenido) o puede ella misma generar ciertos contenidos (participante o generadora de contenidos).

Tabla 1. Clasificación de amenazas y oportunidades del ocio online para personas mayores.

		persona mayor como receptora de contenido	**persona mayor como participante o generadora de contenidos**
Oportunidades	Conocimientos sobre ocio online	Recursos de aprendizaje	Contacto con personas que comparten el mismo interés
	Pertenencia a un grupo	Diversidad de ocio online	Ser invitado o incitado a crear o participar
	Identidad social	Recibir consejos de otros participantes	Redes sociales, intercambio de experiencias

8 Carpenter, B. y Buday, S. (2007). Computer use among older adults in a naturally occurring retirement community. *Computers in Human Behavior, 23*, 3012-3024.

9 De Miguel Molina, M. y Martínez Gómez, M. (2011). A comparative empirical study on Mobile ICT services, social responsibility and the protection of children. *Journal of Science and Engineering Ethics*, Volume 17, Number 2, 245-270.

Amenazas	Comerciales	Promociones no solicitadas, spam	Apropiación de información o datos personales
	Ocio que fomenta la agresividad	Contenidos violentos	Ser acosado, intimidado, ofendido
	Ocio que crea adicción	Información nociva	Autodestructivo, no puede desengancharse

Fuente: Elaboración propia a partir de Livingstone, S. y Haddon, L. (2009). *EU Kids Online: Final report*. LSE, London: EU Kids Online. P. 10.

Si bien los datos de las personas mayores no tienen, conforme a lo establecido en nuestra normativa, la consideración jurídica de «datos especialmente protegidos» *per se*, estos forman parte de una categoría sui generis que podríamos denominar «datos de personas especialmente vulnerables», basada en un criterio subjetivo en función de las personas titulares de los datos y las especiales circunstancias que les caracterizan[10]. Interesa subrayar, a este respecto, la existencia de determinados factores que son consecuencia lógica de la edad avanzada de las personas, tales como un progresivo deterioro físico, sensorial, mental y cognitivo, que convierten a los mayores en un colectivo social de riesgo por su especial fragilidad. Y que, por ende, los hace dignos merecedores de un especial cuidado y protección en su condición de personas especialmente vulnerables. Una vulnerabilidad que aumenta de manera exponencial en la sociedad digital, como consecuencia del desfase generacional.

Por ello para superar con éxito el reto de la protección de datos de las personas mayores en la sociedad del ocio digital es necesaria una estrategia pluridimensional y omnicomprensiva de la problemática de este colectivo social de especial sensibilidad, basada en los siguientes puntos clave:

- El fomento y promoción de acciones de sensibilización que contribuyan a normalizar la cultura de la protección de datos entre las personas mayores y les capaciten para el control de su propia información en el mundo digital.
- El seguimiento sin fisuras de una línea de respeto a la autonomía de la voluntad de las personas mayores, siempre que ello sea legal y fácticamente posible, basada en el consentimiento libre e informado del propio interesado para el tratamiento de los datos que le conciernen.
- La armonización del derecho de información recogido en la normativa sobre protección de datos, erigiendo el cumplimiento de los principios de transparencia y de respe-

10 Gómez-Juárez Sidera, I. y Lara Yuste, F. (2009). Personas mayores en la sociedad de las nuevas tecnologías: la necesidad de navegar hacia un horizonte donde el derecho a la protección de sus datos sea plenamente respetado. *Revista digital Datospersonales.org, 40.* Recuperado 2 de febrero de 2012, en http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142560422023&esArticulo=true&idRevistaElegida=1142557356539&language=es&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales

to del contexto en el mínimo exigible de calidad con respecto a la información que se facilite a las personas mayores sobre el tratamiento de sus datos.

- El respeto exquisito de los principios de finalidad y minimización de los datos como límite infranqueable para los responsables de ficheros o tratamientos específicamente vinculados a personas mayores.
- La implementación de parámetros por defecto respetuosos con el derecho fundamental a la protección de datos en relación a los tratamientos vinculados a personas mayores en el ámbito digital.
- El establecimiento de sanciones cualificadas para inhibir la recogida de datos de personas mayores en forma engañosa o fraudulenta.
- El fomento de iniciativas de autorregulación y la promoción de códigos de conducta, con el fin de facilitar una aplicación efectiva de la normativa sobre protección de datos, teniendo en cuenta las características específicas de los tratamientos vinculados a personas mayores en el ámbito digital.

Debido a las limitaciones del espacio, profundizaremos únicamente sobre aquellas cuestiones que consideramos más transcendentales, sin que ello deba entenderse, en ningún caso, un menosprecio a las restantes, que pueden tratarse en posteriores estudios.

2. PROTECCIÓN DE DATOS DE LAS PERSONAS MAYORES EN LA SOCIEDAD DEL OCIO DIGITAL

2.1. Brecha generacional digital y cultura de la protección de datos

El término «inclusión digital» hace referencia a las medidas destinadas al logro de una sociedad de la información inclusiva, es decir, una sociedad de la información que sea para todos. El objetivo es hacer posible que toda persona que lo desee pueda, a pesar de sus desventajas individuales o sociales, participar plenamente en la sociedad de la información. En este sentido, la Declaración Ministerial de Riga, de 11 de junio de 2006, sobre las «TIC para una sociedad inclusiva», identificó varios grupos a los que debían dirigirse las intervenciones primordialmente, entre ellos el colectivo social de la tercera edad.

En este sentido, Ji et al.[11] subrayan los dos hechos diferenciales que separan a las personas mayores de los jóvenes en relación al uso de las nuevas tecnologías. En primer lugar, su escasa familiaridad con las tecnologías de la información y la comunicación. En segundo lugar, la degradación de las capacidades físicas, sensoriales y cognitivas asociada al envejecimiento levanta significativas barreras de acceso a las citadas tecnologías. Asimismo, estos autores ponen el acento sobre el hecho de que las personas mayores no identifiquen las nuevas tecnologías como elementos estrechamente relacionados con su vida cotidiana como

11 Ji, Y. G. et al. (2010). Older Adults in an Aging Society and Social Computing: A Research Agenda. *International Journal of Human-Computer Interaction, 26 (11-12)*, 1122-1146. doi: 10.1080/10447318.2010.516728

consecuencia de que no hicieron uso de ellas durante su juventud. Así por ejemplo, aunque los servicios de redes sociales en Internet se han incrementado, el número de usuarios mayores sigue siendo bajo en comparación con otros grupos de edad. En un mismo sentido, Nimrod[12] señala que el porcentaje de usuarios de Internet entre las personas mayores de 60 años es todavía mucho menor que entre los grupos de edad más jóvenes (20%-50% vs 70%-90%).

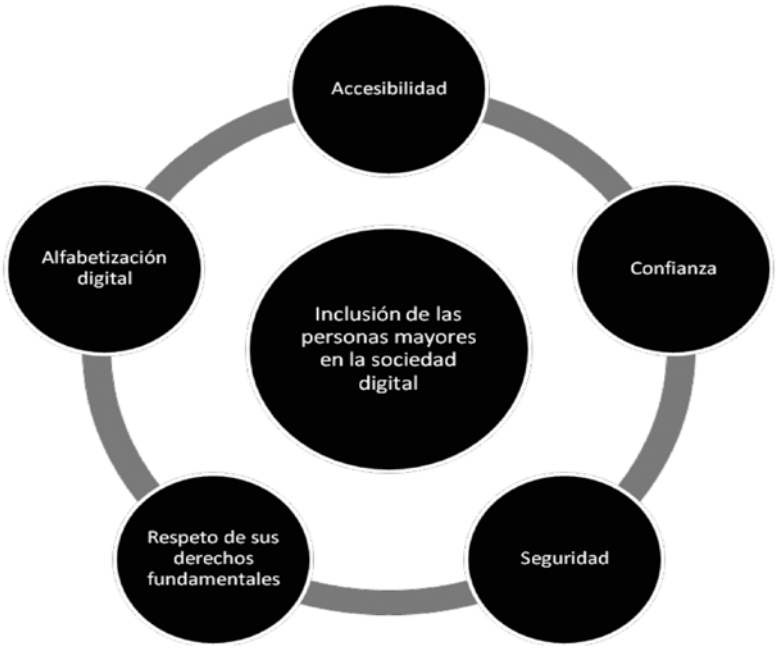
El eje vertebrador de la inclusión de las personas mayores en la sociedad digital en condiciones de igualdad sustantiva, real y efectiva al resto de los ciudadanos, se ha de asentar sobre los irrenunciables criterios vectores de accesibilidad, confianza, seguridad y respeto de sus derechos fundamentales (Figura 1), entendido este último en un sentido amplio, que comprende el respeto del derecho fundamental a la protección de sus datos de carácter personal –consagrado en la trascendental Sentencia 292/2000, de 30 de noviembre, del Tribunal Constitucional–, así como de sus derechos fundamentales al honor y a la intimidad personal y familiar, reconocidos en el artículo 18 de nuestra Constitución.

Asimismo, se presenta un quinto elemento impulsor, aglutinador y dinamizador de todos ellos, clave y determinante para que la inclusión digital de este colectivo social se convierta en una realidad efectiva: la ejecución de una intensa labor divulgativa, informativa y de concienciación, que acerque las ventajas de las nuevas tecnologías a la tercera edad, así como los beneficios potenciales que las mismas pueden aportar a su calidad de vida, y, a su vez, el impulso de actividades educativas y formativas que, desde un punto de vista pedagógico, ayuden a eliminar las barreras consecuencia del desfase generacional que separa a este colectivo de personas respecto del nacimiento de las citadas tecnologías («brecha generacional digital»), desarrollando o, en su caso, potenciando sus conocimientos, competencias y aptitudes «digitales». En suma, a través de lo que se conoce como «alfabetización digital».

Ciertamente, quizá se atenúen los efectos de la que hemos llamado «brecha generacional digital» con el paso del tiempo, si bien intuimos que seguirá siendo necesario un aprendizaje permanente a lo largo de la vida a este respecto. En el caso de las personas mayores, se antoja especialmente interesante el aprendizaje no formal obtenido a través de las diferentes acciones promovidas por las Administraciones Públicas y entidades sin ánimo de lucro con el objeto de favorecer su inclusión en la sociedad digital, así como el aprendizaje informal obtenido a través de sus hijos, nietos e incluso amigos en el marco de las actividades de su vida familiar y de ocio.

12 Nimrod, G. (2010). Seniors' online communities: A quantitative content analysis. *The Gerontologist*, *50*, 382-392. doi:10.1093/geront/gnp141

Figura 1. Elementos necesarios para la inclusión real de las personas mayores en la sociedad digital.



Fuente: Elaboración propia.

A este respecto, el proceso de alfabetización digital del colectivo social de las personas mayores debe ir indisolublemente acompañado de la promoción de las necesarias medidas de sensibilización y divulgación en el terreno de la defensa del derecho fundamental a la protección de sus datos, en pos de normalizar la cultura de la protección de datos entre las personas mayores y proporcionarles las herramientas suficientes para el control de su propia información en el mundo digital. Recordar que, en opinión del Grupo de Trabajo del artículo 29[13], un buen sistema de protección de datos se caracteriza, en general, por el hecho de que los responsables del tratamiento conocen muy bien sus obligaciones y los interesados conocen muy bien sus derechos y medios para ejercerlos[14]. En este sentido, la Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC), en colaboración con la propia

13 El Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo europeo independiente en materia de protección de datos y derecho a la intimidad. Sus cometidos se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.
De su secretaría se encarga la Dirección C (Derechos fundamentales y ciudadanía) de la Comisión Europea, Dirección General de Justicia, B-1049 Bruselas, Bélgica, despacho nº MO 59 02/013.

14 Documento de Trabajo «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE», aprobado el 24 de julio de 1998 por el Grupo de Trabajo del artículo 29.

Agencia Española de Protección de Datos, editó en 2009 una guía de protección de datos específicamente orientada a las personas mayores[15]. Iniciativa que ha de gozar del apoyo de medidas complementarias que garanticen su efectividad, asentamiento y continuidad; consideramos potencialmente efectiva la realización de campañas de sensibilización a través de medios de comunicación *offline* (vgr., prensa escrita, radio, televisión, etc.), en los que la persona mayor se siente más cómoda y segura asimilando el mensaje de manera más eficaz.

Cabe citar a este respecto la reciente publicación por la Agencia de Protección de Datos de la Comunidad de Madrid de un folleto divulgativo sobre protección de datos para personas mayores en el mundo tecnológico del siglo XXI, con la finalidad de su distribución en las Oficinas de Atención al Ciudadano de la Comunidad de Madrid y, a través de la Consejería de Asuntos Sociales, en las residencias de mayores.

2.2. La necesaria armonización del derecho de información

2.2.1. El valor instrumental del derecho de información respecto del principio del consentimiento

El importante Dictamen 15/2011 sobre la definición del consentimiento, del Grupo de Trabajo del artículo 29, afirma que «si se utiliza correctamente, el consentimiento es un instrumento que permite al interesado controlar el tratamiento de sus datos», pero «si se utiliza de forma incorrecta, el control por el interesado resulta ilusorio y el consentimiento deja de ser una base adecuada del tratamiento».

En este sentido, la trascendental Sentencia 292/2000, de 30 de noviembre, del Tribunal Constitucional, que consagró el derecho a la protección de datos de carácter personal como un verdadero derecho fundamental autónomo e independiente del derecho a la intimidad, señala que el derecho fundamental a la protección de datos persigue garantizar a la persona «un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado» (FJ 6). De tal manera, garantiza a los individuos un poder de disposición sobre sus datos, si bien «nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin» (FJ 6). Y profundiza: «el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y

15 Gómez-Juárez Sidera, I. (2009). *Aprenda a proteger sus datos: Guía de protección de datos para personas mayores* (1ª ed.). Madrid: Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC).

cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ 7)» (FJ 6).

En suma, «faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular» (FJ 7). Y «requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos» (FJ 7).

De tal modo, concluye el Tribunal Constitucional, «sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales» (FJ 13).

En lo tocante a este particular, debemos concluir que el principio de información, dotado de una manifiesta significación, identidad y contenido propios, tiene, a su vez, un importante valor instrumental respecto del principio del consentimiento, eje vertebrador en torno al cual se estructura y cohesiona nuestro sistema normativo de protección de datos. Así, el principio de información se constituye en un medio para hacer efectivo el principio del consentimiento, sin el cual éste difícilmente podría existir, careciendo de sentido y eficacia. Información y consentimiento son, en suma, principios íntimamente relacionados, completando y perfeccionando el primero al segundo, de manera que entre los caracteres que definen el propio contenido esencial del principio del consentimiento se encuentra la cualidad de «informado»[16], siendo necesaria la concurrencia de este requisito para que el consentimiento pueda ser considerado conforme a derecho[17]. De ahí la trascendental importancia del principio de información como pilar básico en la configuración jurídica del derecho fundamental a la protección de datos, cuyo fin último es la facultad de la persona de controlar la información concerniente a sí misma y la capacidad de disponer sobre ella.

Una idea compartida por el propio Grupo de Trabajo del artículo 29, que en su Dictamen 15/2011 puntualiza que la obligación de informar es diferente del consentimiento, aunque en muchos casos está obviamente vinculada a éste. De tal manera, «mientras que el consentimiento no siempre sigue al suministro de información, la información siempre

16 El artículo 5.1.d) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, entiende por «consentimiento del interesado»: *«Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen»*.

17 Informe del Gabinete Jurídico de la Unidad de Apoyo al Director de la Agencia Española de Protección de Datos sobre los «Caracteres del consentimiento definido por la LOPD (nivel 4)» (2000).

es necesaria antes del consentimiento». Esto significa en la práctica «que el consentimiento debe ser con conocimiento de causa: un consentimiento «informado» por parte del interesado supone un consentimiento basado en la apreciación y comprensión de los hechos y consecuencias de una acción. El individuo afectado debe contar con información exacta y completa, dada de forma clara y comprensible, sobre todas las cuestiones pertinentes, tal como la naturaleza de los datos tratados, los fines del tratamiento de que van a ser objeto los datos, los destinatarios de los mismos y los derechos del interesado. Esto incluye también el conocimiento de las consecuencias de no consentir el tratamiento de los datos en cuestión».

Así lo entiende también Sánchez Carazo, para quien «El derecho a la información es un derecho raíz, pues sin la información no podemos ejercer el resto de los derechos. Para poder consentir sobre cómo se tratan los datos tenemos que tener una información clara y veraz; si no tenemos información no podemos consentir y si no estamos bien informados ni podemos tomar decisiones, ni podemos ejercer nuestra autonomía y nuestra libertad»[18].

No en vano, la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)[19], que abre una nueva etapa en lo que respecta a la protección de los datos de carácter personal en la Unión Europea, define el «consentimiento del interesado» como «toda manifestación de voluntad, libre, específica, informada y explícita, mediante la que el interesado acepta, ya sea mediante una declaración ya sea mediante una clara acción afirmativa, el tratamiento de datos personales que le conciernen». De tal manera, la condición de «informado» se confirma como nota definidora del consentimiento del interesado para el tratamiento de los datos de carácter personal que le conciernan en la sociedad digital.

Es por ello que una aplicación torticera, discriminatoria o fraudulenta del principio de información comportaría la privación del derecho fundamental de las personas mayores a la protección de sus datos y, por ende, la negación de su propia dignidad, valor jurídico fundamental estrechamente vinculado con aquél. Surge, por tanto, la pregunta de en qué sentido habría de armonizarse, en su caso, este principio para que despliegue toda su eficacia y alcance en relación al tratamiento de los datos de las personas mayores en el mundo digital.

2.2.2. Respeto del contexto

En primer lugar, es importante analizar y respetar el contexto específico en el que se recogen los datos, siendo la edad y grado de alfabetización digital del interesado elementos importantes del mismo. En este sentido, el referido Dictamen 15/2011 del Grupo de Trabajo del artículo 29 recoge que la forma en que se facilite la información al interesado deberá

18 Sánchez Carazo, C. (2009). La protección de datos personales de las personas vulnerables. *Anuario Facultad de Derecho - Universidad de Alcalá II*, 203-227. Alcalá de Henares: Servicio de Publicaciones de la Universidad.

19 COM(2012) 11 final. Bruselas, 25.1.2012.

estar condicionada al contexto en que se produce la recogida de los datos de carácter personal, debiendo aquél ser capaz de entenderla. Concepto sobre el que profundiza la propuesta de la Administración Obama de una Declaración de derechos del consumidor en materia de privacidad[20], según la cual el cumplimiento de las obligaciones derivadas del principio de información ha de ser consecuente con la edad y familiaridad del interesado con las nuevas tecnologías. A este respecto, hemos de recordar los efectos negativos de la denominada «brecha generacional digital» sobre las personas mayores, que, unida a su natural fragilidad, hace de las mismas un colectivo social de riesgo en materia de protección de datos.

Cabe señalar que el Grupo de Trabajo del artículo 29 considera que cuanto más difícil resulte para el interesado supervisar y comprender todos los elementos del tratamiento de datos, mayor debe ser el esfuerzo del responsable para obtener un consentimiento basado en información específica y comprensible. De lo cual parece colegirse la exigencia de un mayor grado de diligencia a los responsables de ficheros o tratamientos específicamente vinculados a personas mayores en el ámbito digital. Por ejemplo, no sería exigible la misma responsabilidad al responsable de una red social específicamente dirigida al colectivo de la tercera edad que al de una biblioteca a la que puedan asociarse personas mayores de 65 años, como consecuencia del contexto en que se produce la recogida de los datos puesto en relación con la finalidad, complejidad y riesgos particulares de los tratamientos inherentes a uno y otro supuesto.

2.2.3. Transparencia

El respeto del contexto es un concepto estrechamente vinculado a la idea de transparencia dentro del marco general de lo que podríamos denominar «calidad de la información» (Figura 2). En este sentido, interesa subrayar que un exceso de información puede, en determinados supuestos, tener un efecto diabólico, conduciendo a su no comprensión. Por ende, lo importante, a nuestro juicio, no es la cantidad de información que se facilite al interesado, sino la calidad de la misma, posibilitando un control efectivo sobre sus propios datos basado en el conocimiento.

Figura 2. La calidad de la información.

Fuente: Elaboración propia.

20 The White House (2012). *Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights*. Recuperado 23 de febrero de 2012, en http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b

El Foro Europeo de Responsables de Privacidad (EPOF)[21], en sus «Comentarios sobre la Revisión de la Directiva de la UE sobre Protección de Datos (Directiva 95/46/CE)»[22], de 31 de julio de 2002, fue pionero en exponer sus preferencias por un único aviso sencillo que las empresas pudiesen usar en sus promociones y en las relaciones e interacciones con sus clientes en los Estados miembros, que proporcionase la información necesaria en un formato coherente y entendible para aquéllos. Asimismo, manifestaron su oposición a la exigencia de requisitos como extensos avisos legales o interminables declaraciones de privacidad, ya que ello podía conducir a que no fuesen leídos y, por lo tanto, a la desprotección de los derechos e intereses de los consumidores relativos a su privacidad.

Idea compartida por Cavoukian, para quien la utilización de «políticas y notificaciones de privacidad largas, complejas e ilegibles, empapadas de jerga jurídica sin directrices ni normalización, con miedo a la responsabilidad y utilizando palabras para eludir responsabilidades»[23] es altamente ineficaz como herramienta de comunicación y no dice nada al público, desanimando a los ciudadanos y a los clientes a leer, sin mencionar la comprensión y la toma de decisiones efectivas e informadas.

En este sentido, la Comunicación de la Comisión Europea sobre «Un enfoque global de la protección de los datos personales en la Unión Europea»[24], señala que «la transparencia es una condición fundamental indispensable para permitir a las personas efectuar un control sobre sus propios datos y para garantizar la protección efectiva de los datos personales. Es pues primordial que los responsables del tratamiento informen a los ciudadanos correcta y claramente, con toda transparencia, para que sepan quién recogerá y tratará sus datos, de qué manera, por qué motivos y durante cuánto tiempo, y cuáles son sus derechos a efectos de acceder, rectificar o suprimir sus datos». La transparencia se basa, a juicio de la Comisión, «en elementos fundamentales, como un acceso fácil a la información, que debe ser fácil de entender, y la utilización de un lenguaje claro y sencillo. Eso es particularmente importante en un medio en línea donde, muy a menudo, las declaraciones de confidencialidad carecen de claridad, son difícilmente accesibles, poco transparentes, y no se ajustan siempre plenamente a las normas vigentes».

El artículo 11[25] de la reciente Propuesta europea de Reglamento general de protección de datos, introduce la obligación para los responsables del tratamiento de ofrecer informa-

21 European Privacy Officers' Forum.

22 Comments on Review of the EU Data Protection Directive.

23 Cavoukian, A. (2006). La nueva generación de privacidad práctica: una evolución. *Revista digital Datospersonales.org, 21.* Recuperado 16 de febrero de 2012, en http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142302837162&esArticulo=true&idRevistaElegida=1142302823894&language=es&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales&urlPage=RevistaDatosPersonales%2FPage%2Fhome_RDP

24 COM(2010) 609 final. Bruselas, 4.11.2010.

25 Artículo 11
Transparencia de la información y la comunicación

ción transparente y de fácil acceso y comprensión. De tal manera, el principio de transparencia recogido exige que toda información dirigida al público o al interesado sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro[26]. También la Resolución de Madrid del año 2009 sobre «Estándares Internacionales de Protección de Datos Personales y Privacidad», señaló que «cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo, y ello en especial en aquellos tratamientos dirigidos específicamente a menores de edad», estableciendo asimismo que cuando los datos de carácter personal sean recogidos en línea a través de redes de comunicaciones electrónicas, dicha obligación se satisfaga mediante la publicación de políticas de privacidad fácilmente accesibles e identificables.

Un principio, el de transparencia, que también ha recogido el plan de la Administración Obama para proteger la privacidad en la era de Internet, a través de la citada propuesta de adopción de una Declaración de derechos del consumidor en materia de privacidad. En este sentido, recoge expresamente, bajo el epígrafe «Transparencia», que «los consumidores tienen derecho a información fácilmente comprensible y accesible sobre privacidad y prácticas de seguridad». La idea subyacente a este principio es capacitar a los consumidores para una comprensión efectiva de los riesgos para su privacidad y un control real sobre sus datos personales.

En suma, el principio de transparencia, de reciente alumbramiento, se presenta consustancial e inherente al trascendental principio de información, muy especialmente en lo que respecta al tratamiento de datos de personas especialmente vulnerables en el mundo digital. Por ende, si bien el artículo 11 del futuro Reglamento europeo de protección de datos hace una referencia expresa a la información dirigida específicamente a los niños, sorprende poderosamente el hecho de que nada se prevea en relación a los criterios de accesibilidad para las personas mayores y las personas con discapacidad a la información relativa al tratamiento de sus datos personales. Máxime desde nuestro lógico entendimiento de las personas mayores como un colectivo social de riesgo en materia de protección de datos.

Consideramos que algo debería haberse previsto a este respecto, entendiendo en todo caso que la información que se facilite a las personas mayores ha de ser fácilmente accesible y claramente visible (ubicación, tipo y tamaño de los caracteres, etc.), debiendo utilizarse un lenguaje sencillo, claro y adaptado a la realidad sociocultural de sus destinatarios, así como complementarse el texto con presentaciones gráficas o sonoras cuando ello facilite la comprensión del mismo. Asimismo, sería oportuno facilitar a los interesados un medio de contacto sencillo y gratuito (vgr., un número de teléfono gratuito), a fin de poder formular

1. El responsable del tratamiento aplicará políticas transparentes y fácilmente accesibles por lo que respecta al tratamiento de datos personales y al ejercicio de los derechos de los interesados.
2. El responsable del tratamiento facilitará al interesado cualquier información y comunicación relativa al tratamiento de datos personales, en forma inteligible, utilizando un lenguaje sencillo, claro y adaptado al interesado, en particular para cualquier información dirigida específicamente a los niños.

26 Considerando 46.

cuantas preguntas fuesen necesarias en orden a decidir de manera informada y consciente sobre el tratamiento de sus datos.

Esta idea es algo que ya expuso el propio Grupo de Trabajo del artículo 29 en su no tan reciente Dictamen 10/2004 sobre una mayor armonización de las disposiciones relativas a la información, y que consideramos de especial utilidad en el ámbito de las personas mayores. Entendemos que ello también contribuiría a impedir la recogida de datos de personas mayores en forma engañosa o fraudulenta.

Asimismo, la necesidad de un lenguaje claro y llano que las personas mayores puedan comprender con facilidad adquiere una singular relevancia en el mundo digital, como consecuencia de la denominada «brecha generacional digital», que hace de éste un colectivo social especialmente vulnerable. La realidad nos enseña que términos como *cookie*, dirección IP, *cloud computing*, RFID o geolocalización son completamente ajenos a las personas mayores. Asimismo, la utilización de conceptos jurídicos abstrusos tampoco debería tener cabida en una política de privacidad que aspire a ser fácilmente comprensible para un usuario medio, con independencia de su edad.

Además, el hecho de complementar el texto con representaciones gráficas o sonoras no es una cuestión baladí, tomando en consideración el progresivo deterioro físico, sensorial, mental y cognitivo propio de las personas de edad avanzada. Así, por ejemplo, la inserción de un video o una presentación explicativos en la política de privacidad de una página de Internet específicamente dirigida a personas mayores puede facilitar la comprensión del texto a aquéllas con determinados tipos de deficiencias cognitivas. De igual manera, entendemos que una explicación sonora del texto contribuye a facilitar el acceso al mismo a las personas mayores con deterioro visual.

2.3. Fomento de iniciativas de autorregulación y promoción de códigos de conducta

En el sistema español de protección de datos la autorregulación tiene unos determinados límites que vienen impuestos por el reconocimiento de la naturaleza de derecho fundamental del derecho a la protección de datos de carácter personal derivado de los arts. 18.1 y 18.4 CE.

El artículo 53.1 CE establece un principio de reserva de ley para el desarrollo y regulación de los derechos y libertades reconocidos en el Capítulo II del Título I de la Constitución, de manera que sólo por Ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades. Asimismo, el artículo 81.1 CE establece un principio de reserva de ley orgánica para el desarrollo de los derechos fundamentales y de las libertades públicas, exigiendo para su aprobación mayoría absoluta del Congreso.

De lo anterior se colige que la autorregulación no puede aspirar a ser un sustituto de la regulación en nuestro sistema de protección de datos porque hay determinados aspectos del citado derecho fundamental en los cuales sencillamente no tiene cabida. Ésta es una realidad constitucional innegable, motivo por el cual no es admisible la adopción de un sistema de protección de datos de corte anglosajón basado únicamente en la autorregulación, tal como

señala Piñar Mañas[27]. Ahora bien, lo anterior no impide en absoluto dar entrada a la autorregulación, dentro de sus propios límites, en relación a los tratamientos específicamente vinculados a personas mayores en el contexto digital.

Señalar, en este sentido, que la propia Agencia Española de Protección de Datos[28] ha celebrado la decisión de la Comisión Europea de fomentar las iniciativas de autorregulación y la promoción de códigos de conducta en materia de protección de datos de carácter personal. Estos códigos de conducta suponen un paso adelante para que los diferentes sectores se adapten a las particularidades de la protección de datos, teniendo en cuenta además el dinamismo de algunos de ellos. De tal manera, a criterio de la citada autoridad, los códigos de conducta pueden suponer una mayor facilidad para adaptarse a los cambios y un instrumento de valor añadido tanto para los sectores como para los ciudadanos, si bien estos sistemas de autorregulación deben garantizar la representación del sector, gozar de credibilidad y garantizar la actualidad de sus disposiciones. Asimismo, sería importante que existiera un mecanismo claro de acreditación de la adhesión a estos instrumentos, de forma que exista una transparencia y sean identificadas las entidades comprometidas.

De igual modo, a juicio de la Agencia, sería preciso que la normativa sobre protección de datos recogiera elementos que aseguren el cumplimiento de los códigos de conducta mediante la posibilidad de realizar auditorías eficientes, creando sistemas de control de cumplimiento y respeto por la normativa y pudiendo actuar ante eventuales incumplimientos de las normas del código y de la legislación vigente. Estos sistemas habrían de recoger mecanismos internos de control que impliquen consecuencias para aquellas empresas que incumplan lo en ellos estipulado, no sustituyendo en ningún caso las competencias de las autoridades de protección de datos ni las sanciones que eventualmente pudieran imponer.

En opinión de Esteve Pardo, «la complejidad que suscita la entrada de la autorregulación en la órbita de los derechos y valores fundamentales es normalmente una complejidad de orden ético. Las cuestiones se plantean más allá de lo que establecen las normas, que tampoco habrían de pronunciarse por lo demás con sus enunciados generales y abstractos, sobre lo que son situaciones particulares con su problemática propia. En unos casos se trata de adaptar a la realidad las determinaciones y exigencias del Derecho positivo; en otros casos se sigue una orientación positiva que mira más allá del respeto a unos derechos y valores para plantear una mayor exigencia ética»[29]. En el caso concreto que nos ocupa, ambas vertientes de la autorregulación confluyen, a nuestro juicio, en una única vía, con el doble objeto de

27 Piñar Mañas, J. L. (2010). Códigos de conducta y espacio digital. Especial referencia a la protección de datos. *Revista digital Datospersonales.org, 44.* Recuperado 17 de febrero de 2012, en http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142584054265&esArticulo=true&idRevistaElegida=1142582100339&language=es&pag=3&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales

28 Contribución de la Agencia Española de Protección de Datos a la Consulta de la Comisión sobre un enfoque global de la protección de datos personales en la Unión Europea.

29 Esteve Pardo, J. (2008). El reto de la autorregulación o cómo aprovechar en el sistema jurídico lo que se gesta extramuros del mismo. Mito y realidad del caballo de Troya. En Luis Arroyo Jiménez y

adecuar lo establecido en la normativa sobre protección de datos a las circunstancias únicas que caracterizan a las personas mayores, adoptando, asimismo, un *plus* ético y de responsabilidad en relación al tratamiento de los datos de este colectivo especialmente vulnerable y de gran sensibilidad social.

Por tanto, no se trataría de sustituir a las normas que regulan el derecho a la protección de datos sino de complementarlas, es decir de ir más allá de lo que la norma recoge[30].

3. CONCLUSIONES

Las personas mayores son un colectivo especialmente sensible a la protección de sus datos en la sociedad digital debido a la «brecha tecnológica» que se da por el salto generacional. Sin embargo, no parece que hayan recibido tanta atención como, por ejemplo, los menores de edad.

En este sentido, deberían tomarse medidas especiales para que las empresas que ofertan servicios de ocio a este colectivo sean capaces de cumplir tanto su responsabilidad legal como social para que la información sobre el uso que se hace de sus datos personales sea de calidad, posibilitando el control de los mismos sustentado en el ejercicio de la autonomía de la voluntad de las personas mayores.

4. BIBLIOGRAFÍA

Carpenter, B. y Buday, S. (2007). Computer use among older adults in a naturally occurring retirement community. *Computers in Human Behavior, 23*, 3012-3024.

Cavoukian, A. (2006). La nueva generación de privacidad práctica: una evolución. *Revista digital Datospersonales.org, 21.* Recuperado 16 de febrero de 2012, en http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142302837162&esArticulo=true&idRevistaElegida=1142302823894&language=es&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales&urlPage=RevistaDatosPersonales%2FPage%2Fhome_RDP

De Miguel Molina, M. y Martínez Gómez, M. (2011). A comparative empirical study on Mobile ICT services, social responsibility and the protection of children. *Journal of Science and Engineering Ethics*, Volume 17, Number 2, 245-270.

Adán Nieto Martín (ed.), Autorregulación y sanciones (1.ª ed., p. 39-51) Valladolid: Editorial Lex Nova, S.A.

30 De Miguel Molina, M. y Martínez Gómez, M. (2011). A comparative empirical study on Mobile ICT services, social responsibility and the protection of children. *Journal of Science and Engineering Ethics*, Volume 17, Number 2, 245-270.

Esteve Pardo, J. (2008). El reto de la autorregulación o cómo aprovechar en el sistema jurídico lo que se gesta extramuros del mismo. Mito y realidad del caballo de Troya. En Luis Arroyo Jiménez y Adán Nieto Martín (ed.), *Autorregulación y sanciones* (1.ª ed., p. 39-51) Valladolid: Editorial Lex Nova, S.A.

Gómez-Juárez Sidera, I. (2009). *Aprenda a proteger sus datos: Guía de protección de datos para personas mayores* (1ª ed.). Madrid: Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC).

Gómez-Juárez Sidera, I. y Lara Yuste, F. (2009). Personas mayores en la sociedad de las nuevas tecnologías: la necesidad de navegar hacia un horizonte donde el derecho a la protección de sus datos sea plenamente respetado. *Revista digital Datospersonales.org, 40.* Recuperado 2 de febrero de 2012, en http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142560422023&esArticulo=true&idRevistaElegida=1142557356539&language=es&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales

Ji, Y. G. et al. (2010). Older Adults in an Aging Society and Social Computing: A Research Agenda. *International Journal of Human-Computer Interaction, 26 (11-12)*, 1122-1146. doi: 10.1080/10447318.2010.516728

Livingstone, S. y Haddon, L. (2009). *EU Kids Online: Final report*. LSE, London: EU Kids Online.

Nimrod, G. (2010). Seniors' online communities: A quantitative content analysis. *The Gerontologist*, *50*, 382-392. doi:10.1093/geront/gnp141

Nimrod, G. (2011). The Fun Culture in Seniors' Online Communities. *The Gerontologist*, *51 (2)*, 226-237. doi: 10.1093/geront/gnq084

Piñar Mañas, J. L. (2010). Códigos de conducta y espacio digital. Especial referencia a la protección de datos. *Revista digital Datospersonales.org, 44.* Recuperado 17 de febrero de 2012, en http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142584054265&esArticulo=true&idRevistaElegida=1142582100339&language=es&pag=3&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales

Sánchez Carazo, C. (2009). La protección de datos personales de las personas vulnerables. *Anuario Facultad de Derecho - Universidad de Alcalá II*, 203-227. Alcalá de Henares: Servicio de Publicaciones de la Universidad.

Stebbins, R. A. (1997). Casual leisure: A conceptual statement. *Leisure Studies*, *16*, 17-25. doi: 10.1080/026143697375485

The White House (2012). *Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights*. Recuperado 23 de febrero de 2012, en http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b

BALANCING INTELLECTUAL PROPERTY AGAINST DATA PROTECTION: A NEW RIGHT'S WAVERING WEIGHT

Gloria González Fuster
Researcher at Vrije Universiteit Brussel (VUB),
Research Group on Law Science Technology & Society (LSTS)

ABSTRACT: National authorities imposing on Internet service providers the systematic processing of personal data in the name of the protection of intellectual property do not strike a fair balance between the interest of copyright holders in ensuring their right to intellectual property, on the one hand, and the right to personal data protection of those affected by the data processing, on the other. This idea has been sustained twice by the Court of Justice of the European Union (EU), in its judgements of 24 November 2011 for Case C-70/10, Scarlet Extended SA v SABAM, and of 16 February 2012, for Case C 360/10, SABAM v Netlog NV. The postulate, however, is grounded on an unprecedented understanding of the right to the protection of personal data as a EU fundamental right, and on an innovative approach to the balancing exercise between such right and any other interests. This paper first introduces both judgements. Second, it places them in the context of the Luxembourg Court's case law on the protection of personal data, emphasising its infrequent recognition of the existence of a EU right to the protection of personal data as safeguarded by Article 8 of the EU Charter of Fundamental Rights, and its changing interpretation of the object of EU data protection law. Third, it describes the Court's tendency to affirm the need to balance the applicable fundamental rights, while deferring such balancing. Against this background, it describes the most striking particularities of the mentioned judgements.

KEYWORDS: personal data protection, privacy, intellectual property, European Union, fundamental rights.

National authorities imposing on Internet service providers the systematic processing of personal data in the name of the protection of intellectual property do not strike a fair balance between the interest of copyright holders in ensuring their right to intellectual property, on the one hand, and the right to personal data protection of those affected by the data processing, on the other. This statement, pronounced twice by the Court of Justice of the European Union (EU) in a short lapse of time, represents a powerful judicial contribution to a debate of significant relevance nowadays. The postulate, however, is grounded on an unprecedented understanding of the right to the protection of personal data as a EU fundamental right, and on a groundbreaking approach to the balancing exercise between such right and any other interests.

This paper first introduces the judgments of the EU Court of Justice where this approach has materialised. Second, it places them in the wider context of the still embryonic Court's case law on the EU fundamental right to the protection of personal data, a right without equivalent in the common constitutional traditions of Member States, or in the European Convention

on the Protection of Human Rights and Fundamental Freedoms (ECHR). Third, it analyses the specificity of the balancing as upheld by the Court in the rulings at stake, arguing that the Court's positioning appears to vary depending on the contexts in which it is called upon to examine the interpretation and application of EU personal data protection.

1. INTRODUCING *SCARLET* AND *NETLOG*

The pronouncements of the Luxembourg-based EU Court of Justice were issued in the context of two separate references for preliminary rulings, submitted by two different Belgian courts. They both concerned demands of the *Société belge des auteurs, compositeurs et éditeurs* ('SABAM') for injunctions to impose on private companies a generalised monitoring of the use of Internet services. In one case, the monitoring was to be forced upon the Internet service provider (ISP) Scarlet Extended SA ('Scarlet'), provider of Internet access. In the other, the SABAM wished to inflict similar obligations upon Netlog, owner of an online social networking platform.

1.1. Scarlet v Sabam

A first judgment was delivered in November 2011, for the *Scarlet v Sabam* case (hereafter, *'Scarlet'*).[1] The referring court had asked the EU Court of Justice for guidance on the interpretation of EU law applicable in proceedings between Scarlet and the SABAM, concerning Scarlet's refusal to install a system for filtering electronic communications which use file-sharing software ('peer-to-peer'), despite a previous injunction in this sense.[2] The system would involve, in the name of the insurance of the right to intellectual property, the systematic processing of IP addresses.[3] In Scarlet's view, the injunction was contrary to Belgian law implementing EU law because it equalled the imposition of a general obligation to monitor communications on its network, inasmuch as any system for blocking or filtering peer-to-peer traffic necessarily requires general surveillance of all communications passing through the network.[4]

The Court of Justice acknowledged that the right to intellectual property is to be protected, but it nuanced that it is not an absolute right, and that it must, thus, be balanced against other fundamental rights when necessary.[5] In line with its 2008 judgment for the *Promusicae v Telefónica ('Promusicae')* case,[6] the Court stated that, in the context of measures

1 Judgement of the Court (Third Chamber), 24 November 2011, Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM).*

2 *Ibidem*, § 2.

3 *Ibid*., § 51.

4 *Ibid*., § 25.

5 *Ibid*., § 44.

6 Judgment of the Court (Grand Chamber), 29 January 2008, Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*. On this ruling, see: González Gozalo, Alfonso

adopted to protect copyright holders, national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals affected by such measures. The latter include, the Court specified, the freedom to conduct business, the freedom to receive and impart information, and the right to the protection of personal data.[7]

Observing that the monitoring obligations had no limitation in time, that they were directed to all future infringements and were intended to protect not only existing works but also works still to be created,[8] requiring the installation of a complicated, costly, and permanent computer system, the Court of Justice considered that they would result in «*a serious infringement*» of Scarlet's freedom to conduct its business[9] and that, therefore, they did not respect the requirement that a fair balance be struck between the right to the protection of intellectual property and the freedom to conduct business.[10] As the system might not distinguish adequately between unlawful and lawful content, the Luxembourg Court also found that it could undermine freedom of information,[11] and that, consequently, fair balance had not been struck either with the freedom to receive and impart information.[12]

The Court of Justice, moreover, taking into account that the filtering system would involve the systematic processing of IP addresses, which are to be regarded as «*protected personal data*»,[13] concluded that imposing such a system would not respect the requirement that a fair balance be struck with the right to protection of personal data[14] as safeguarded by Article 8 of Charter of Fundamental Rights of the EU.[15]

(2008). El conflicto entre la propiedad intelectual y el derecho a la portección de datos de carácter personal en las redes *peer to peer. Pe. i: Revista de propiedad intelectual*, 28, 13-68. González Vaqué, L. (2008). El TJCE se pronuncia sobre la obligación de comunicar datos personales a fin de garantizar la protección de los derechos de autor en un procedimiento civil: la sentencia «Promusicae». *Aranzadi Unión Europea, año 34, mayo*(5), 5-14; Groussot, X. (2008). Case C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU,* Judgement of the Court (Grand Chamber) of 28 January 2008: Rock the KaZaA: Another Clash of Fundamental Rights. *Common Market Law Review*, 45, 1745-1766. See also: Order of the Court (Eighth Chamber) of 19 February 2009, Case C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH;* and Ordóñez Solís, D. (2011). Las descargas ilegales en Internet: el contexto jurídico europeo de la *Ley Sinde*. *Unión Europea Aranzadi, año 2011 - noviembre*(11), 7-20.

7 *Scarlet*, § 45.

8 *Ibid*., § 47.

9 *Ibid*., § 48.

10 *Ibid*., § 49.

11 *Ibid*., § 52.

12 *Ibid*., § 53.

13 *Ibid*., § 51.

14 Idem.

15 *Scarlet*, § 50.

1.2. Sabam v Netlog

A judgment echoing this approach was delivered in February 2012, for the *SABAM v Netlog* (*'Netlog'*) case,[16] concerning a reference for a preliminary ruling raised in proceedings between the SABAM and Netlog NV ('Netlog'). Here was at stake an injunction for the introduction of a system for filtering information stored on Netlog's social networking platform. In its ruling, the Court of Justice, following a reasoning very similar to the one in *Scarlet*, equally concluded that in adopting the injunction obliging the hosting service provider to install the contested filtering system the national court concerned would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on one side, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other.[17]

This time, the Court founded its assessment related to the unfairness of the balance between the right to intellectual property and the right to protection of personal data on the fact that the filtering system would involve the systematic processing of information connected with the profiles of the social network's users, considered «*protected personal data*».[18]

The *Netlog* judgement thus consolidated the Court's case law inaugurated in *Scarlet* according to which Article 8 of the Charter safeguards a fundamental right to the protection of personal data, which is not fairly balanced with copyright holders' rights when a system requiring the systematic processing of personal data is imposed in the name of the protection of intellectual property. Until then, the Court had very rarely acknowledged the existence of a EU right to the protection of personal data, and had been extremely reluctant to operate any balance between conflicting rights necessary to the implementation of EU data protection law.

2. A NEW RIGHT IN THE MAKING

The right to personal data protection[19] can be described as an emerging right. It is now formally present in EU primary law, but the EU Court of Justice, maximum interpreter of EU law, has not yet clearly drawn up its contours, or described its essential content.

---

16 Judgement of the Court (Third Chamber), 16 February 2012, Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV.*

17 *Ibid*., § 51.

18 *Ibid*., § 49.

19 On the EU fundamental right to the protection of personal data, see: Arenas Ramiro, M. (2006). *El derecho fundamental a la protección de datos personales en Europa.* Valencia: Tirant Lo Blanch; Siemen, B. (2006). *Datenschutz als europäisches Grundrecht*. Berlin: Duncker & Humblot; Coudray, L. (2010). *La protection des données personnelles dans l'Union européenne: Naissance et consécration d'un droit fondamental*. Berlin: Éditions universitaires européennes.

2.1. The innovation of the Charter

The EU right to personal data protection was first mentioned as such in 2000 in the EU Charter of Fundamental Rights, an instrument rendered legally binding (in a slightly modified version)[20] only in December 2009, with the entry into force of the Lisbon Treaty.[21] Article 8(1) of the Charter establishes that «(*e)veryone has the right to the protection of personal data concerning him or her*». Article 8(2) states that «(*s)uch data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*», and that «(*e)veryone has the right of access to data which has been collected concerning him or her, and the right to have it rectified*». Finally, Article 8(3) determines that «*compliance with these rules shall be subject to control by an independent authority*».[22]

The inclusion of this right in the Charter represented a remarkable novelty in the EU fundamental rights landscape. Until then, only a few Member States had witnessed the advent of a similar right to the protection of personal data in their own legal orders. The Strasbourg-based European Court of Human Rights had been providing judicial protection against the automated processing of data in the name of another right – namely, the right to respect of private life, as established by Article 8 of the ECHR, and as developed in 1981 by the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ('Convention 108').[23]

To justify the unprecedented incorporation of the right to personal data in the Charter, its drafters mentioned the need to up-date existing catalogues of rights in the light of technological progress, and many legal sources: notably, said Article 8 of the ECHR and the case law of the European Court of Human Rights thereof, as well as Convention 108, and various EU provisions adopted in the 1990s, including both primary and secondary law. None of these sources, however, had ever mentioned the existence of a right to data protection as an autonomous fundamental right, different from the right to respect for private life. Its recognition as such in the Charter represented thus a considerable breakthrough.

2.2. Lack of straightforward reception in the case law

Until recently, the EU Court of Justice had not openly embraced this evolution.[24] It was only in 2008 when it first acknowledged that Article 8 of the Charter established a right

20 Charter of Fundamental Rights of the European Union, *Official Journal of the European Union C 83,* 30.3.2010, 389-403.

21 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, *Official Journal of the European Union,* C 306, 17.12.2007, 1-271.

22 On this Article, see: Ruiz Miguel, C. (2003). El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Unión Europea: Análisis crítico. *Revista de Derecho Comunitario Europeo*, 7(14), 7-43.

23 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28 January 1981, European Treaty Series No. 108.

24 On the case law of the EU Court of Justice on personal data protection, see, notably: De Hert, P. and S. Gutwirth (2009). Data Protection in the Case Law of Strasbourg and Luxembourg: Constitution-

to the protection of personal data. In the 2008 *Promusicae* judgement, indeed, observing that Directive 2002/58/EC[25] (adopted in 2002, after the proclamation of the Charter) referred to such provision in its Preamble, the Court noted: «*Article 8 of the Charter expressly proclaims the right to protection of personal data*».[26] Such pioneering recognition, nevertheless, was of little effect, as the rest of the judgement replaced any possible mention of such right with references to the right to respect for private life.[27]

2.2.1. The moving object of data protection law

Most often, even after the *Promusicae* ruling, the Court of Justice has been dealing with the interpretation of EU data protection law without making any reference to the existence of a EU fundamental right to data protection. The right is crucially absent from the major EU data protection legal instrument ever approved, adopted in 1995 (before the Charter's proclamation in 2000): Directive 95/46/EC,[28] the object of which is, according to its own words, to ensure that Member States «*protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*», while forbidding any restrictions of the «*free flow of personal data between Member States*».[29]

The Luxembourg Court has many times recalled those words to frame its interpretation of Directive 95/46/EC. It did so, for instance, in the December 2008 judgement for the *Satamedia* case,[30] where the right to the protection of personal data was not quoted at all, even if Advocate

---

alism in Action. In Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile De Terwangne & Sjaak Nouwt (eds.), *Reinventing Data Protection?* (pp. 3-44). Dordrecht: Springer; Oliver, P. (2009). The protection of privacy in the economic sphere before the European Court of Justice. *Common Market Law Review,* 46, 1443-1483.

25 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal of the European Communities,* L 201, 31.7.2002, 37-47.

26 *Promusicae*, § 64.

27 *Ibid*., § 65. A comparable phenomenon can be perceived in the Opinion of Advocate General Kokott for Case C-275/06, delivered on 18 July 2007, as she mentions the recognition of the fundamental right to data protection in Article 8 of the Charter (§ 51), but places her argumentation under the light of Article 8 of the ECHR (§ 52 and following).

28 Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Communities* L 281, 23.11.1995, 31-50.

29 Article 1 of Directive 95/46/EC.

30 Judgment of the Court (Grand Chamber), 16 December 2008, Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy,* § 52. See also: Docquir, B. (2009). Arrêt *Satamedia*: la (re)diffusion d'informations publiques dans les médias et les exigences de la protection des données. *Revue européenne de droit à la consommation*, 2-3, 560-581; and Hins, W. (2010). Case C-73/07,

General Kokott had referred to it in her Opinion for the case.[31] In the 2009 *Rijkeboer* judgement,[32] the Court of Justice asserted that Directive 95/46/EC served primarily the protection of privacy and as a consequence the protection of personal data, as highlighted in its Preamble and as allegedly many times emphasised by its own case law.[33] Likewise, it failed to make any allusion to the right to data protection. The 2010 judgement for the *Bavarian Lager* case, despite being directly concerned with asserting the specificity of EU data protection law compared to the content of Article 8 of the ECHR, does not allude either to Article 8 of the Charter.[34]

The Court of Justice has nonetheless mentioned again the EU right to personal data protection. In its 2011 ruling for *Deutsche Telekom AG v Bundesrepublik Deutschland* (*'Deutsche Telekom*'),[35] concerning a reference for preliminary ruling related partially to the interpretation of Directive 2002/58/EC, the Court did not only acknowledge once more such existence, but even asserted that Directive 95/46/EC, later developed by Directive 2002/58/EC, «*is designed to ensure, in the Member States, observance of the right to protection of personal data*«.[36]

The *Deutsche Telekom* judgement was however not deprived of unclear passages. The Luxembourg Court appeared to locate the core content of the right to personal data protection exclusively in the first paragraph of Article 8 of the Charter,[37] subsequently emphasised that such right is not absolute right but must be considered in relation to its function in society,[38] and seemed to situate the description of the manner in which such consideration is to take place in the second paragraph of the Charter's Article 8.[39]

Tietosuojavaltuutettu v. Stakunnan Markkinapörssi Oy and Satamedia Oy, judgment of the Grand Chamber of 16 December 2008, not yet reported. *Common Market Law Review*, 47, 215-233.

31 With a reference to the Promusicae judgement (Opinion of Advocate General Kokott for Case C-73/07, delivered on 8 May 2008, § 40).

32 Judgment of the Court (Third Chamber), 7 May 2009, Case C-553/07, *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer.*

33 *Ibid.*, § 47. The Advocate General giving Opinion for the case had provided a peculiar reading of Article 8 of the Charter, which in his words codified the right to privacy, which had previously found a legislative expression in Directive 95/46/EC (see: Opinion of Advocate General Ruiz-Jarabo Colomer for Case C-553/07, delivered on 22 December 2008, § 8)

34 Judgement of the Court (Grand Chamber), 29 June 2010, Case C-28/08 P, *European Commission v The Bavarian Lager Co. Ltd.*

35 Judgement of the Court (Third Chamber), 5 May 2011, Case C-543/09, *Deutsche Telekom AG v Bundesrepublik Deutschland.*

36 *Ibid.*, § 50.

37 *Ibid.*, § 49. The Court had also referenced only Article 8(1) of the Charter, instead of Article 8 of the Charter as a whole, in its mention of the right to the protection of personal data in *Schecke* (§ 47). On this approach, see: González Fuster, G. and R. Gellert (2012). The fundamental right of data protection in the European Union: in search of an uncharted right. *International Review of Law, Computers & Technology,* 26(1), 73-82.

38 *Deutsche Telekom*, § 51.

39 *Ibid.*, § 52.

2.2.2. The right to respect for private life with regard to the processing of personal data

A judgement illustrating many of the hesitations of the Luxembourg Court as regards the current framing of the protection of personal data in EU law is its 2010 ruling for the *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen ('Schecke')* case,[40] concerning a reference for a preliminary ruling related to the interpretation of EU law, raised in the course of proceedings regarding the applicants' opposition to the publication on a public Internet site of data about them as recipients of EU funds.

In its preliminary observations, the EU Court of Justice noted that the referring court maintained that the publication of the beneficiaries' data constituted an unjustified interference with the fundamental right to the protection of personal data referring essentially to Article 8 of the ECHR.[41] Pointing out that the Charter enjoys legally binding force,[42] the Court of Justice held that it had to interpret the EU law at stake preferably not from the perspective of the ECHR, but rather in the light of the Charter,[43] and thus brought about its Article 8, on the right to protection of personal data.[44] Immediately, however, the Court added that this fundamental right to the data protection «*is closely connected with the right to respect of private life expressed in Article 7 of the Charter*».[45]

The Court of Justice underlined then that the right to data protection is not absolute but must be considered in relation to its function in society,[46] and that this consideration must rely on, in addition to the wording of Article 8 of the Charter itself,[47] the content of Article 52(1) of the Charter,[48] describing the conditions for legitimate limitations of the Charter's rights. Mentioning also Article 52(3),[49] which establishes that the Charter's rights corresponding to ECHR rights must be interpreted similarly, it concluded that there would exist a «*right to respect for private life with regard to the processing of personal data*», recognised jointly by Article 7 and 8 of the Charter, the content of which it described as simply matching the Strasbourg case law on the applicability of Article 8 of the ECHR to the processing of data related to

40 Judgement of the Court (Grand Chamber), 9 November 2010, Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*. On this judgement, see: Bobek, M. (2011). Joined Cases C-92 & C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert*, Judgement of the Court of Justice (Grand Chamber) of 9 November 2010, nyr. *Common Market Law Review*, 48, 2005-2022.

41 *Ibid*., § 44.

42 *Ibid*., § 45.

43 *Ibid*., § 46.

44 More precisely, the Court mentions Article 8(1) of the Charter.

45 *Schecke*, § 47.

46 *Ibid*., § 48.

47 *Ibid*., § 49.

48 *Ibid*., § 50.

49 *Ibid*., § 51.

individuals. As a matter of fact, the core of the Court's judgement, structured around the determination of the existence of an interference with a protected right and of an assessment of the justification of such interference, is directly inspired in Strasbourg's case law.[50]

One of the striking aspects of the *Schecke* judgement is the detour taken by the Luxembourg Court to distance itself from the framing of personal data protection as part of the right to respect for private life of Article 8 of the ECHR, which, through its reading of the Charter, nevertheless took it back to the interpretation of Article 8 of the ECHR. In the course of such digression, furthermore, the Court invented a notion, the «*right to respect for private life with regard to the processing of personal data*», allegedly protected jointly by Article 7 and 8 of the Charter. This expression appeared again in a 2011 ruling, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD).[51]

As the *Schecke* judgement shows, the question of framing data protection law under Article 8 of the ECHR or under Article 8 of the Charter, or under both, is not only of theoretical interest, but has also consequences for the interpretation and application of EU law. Affirming the existence of a EU fundamental right to data protection opens up the questions of how should it be construed, when and how can it be restricted, and how and by whom can it be balanced, when necessary, against any other interest or right.

3. BALANCING AN ELUSIVE RIGHT

Fundamental rights can be subject to balancing operations in various contexts. All fundamental rights that are not absolute can be restricted or limited, and, in the assessment of the legitimacy of such restrictions, must always take place a balancing of the fundamental right itself against any other interest pursued by the limitation. Moreover, the insurance of a fundamental right might need to be balanced with the need to protect other interests or rights.[52] These two basic scenarios are not clearly delimited, as sometimes a restriction will be founded precisely in the need to protect another fundamental right, also leading to a balancing between rights.

3.1. Disparate balancing operations in the context of EU data protection law

The EU Court of Justice started developing its case law on data protection law and the balancing of different interests and rights many years before it acknowledged the existence of a EU fundamental right to data protection.

---

50 *Ibid*., § 52-89.

51 Judgement of the Court (Third Chamber) of 24 November 2011, Joined Cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)* and *Federación de Comercio Electrónico y Marketing Directo (FECEMD)* (C-469/10) v Administración del Estado, § 42.

52 Piñar Mañas, J. L. (2003). El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas. *Cuadernos de Derecho Público*, 19-20(mayo-diciembre), p. 58.

3.1.1. Deferring the balancing

Two important decisions were delivered in 2003. First, the *Rundfunk* [53] judgement, which regarded Austrian legislation requiring the communication of data on employees' income. In its ruling, the EU Court of Justice had to provide guidance on the interpretation of an Article of Directive 95/46/EC allowing Member States to derogate from some of its provisions in certain cases.[54] Arguing that Directive 95/46/EC had as principal aim to ensure the free movement of personal data, but that it also mandated Member States to protect fundamental rights, and in particular the right to privacy,[55] the Court maintained that to do so it was necessary to ascertain, from the point of view of Article 8 of the ECHR, whether the legislation at issue provided for an interference with private life, and, if so, whether it was justified.[56] The Luxembourg Court proceeded to such an examination relying on the case law of the European Court of Human Rights, which insists on the need for interferences to be proportionate to the aim pursued, thus leading it to identify as key the need to balance Austria's interest in ensuring the best use of public funds against the seriousness of the interference with the right of the persons concerned to respect for their private life.[57] The specific assessment of such balancing in the issue at stake was left to the national court.[58]

Second, in the judgement for the *Bodil Lindqvist* ('*Lindqvist')* case,[59] concerning a Swedish catechist who had published information on Internet about her colleagues,[60] the Court of Justice had to examine the question of whether some provisions of Directive 95/46/EC could be interpreted as a restriction conflicting with freedom of expression or other freedoms or rights.[61] In its answer, the Court underlined that Directive 95/46/EC aimed at both insuring the free movement of personal data in the EU and the safeguarding of fundamental rights,[62] but stated that it was primarily at the stage of the application in individual cases of the national measures implementing Directive 95/46/EC that a balance must be found

53 Judgment of the Court of 20 May 2003, Joined cases C-465/00, C-138/01 and C-139/01, *Rechnungshof (C-465/00) and Österreichischer Rundfunk, Wirtschaftskammer Steiermark, Marktgemeinde Kaltenleutgeben, Land Niederösterreich, Österreichische Nationalbank, Stadt Wiener Neustadt, Austrian Airlines, Österreichische Luftverkehrs-AG, and between Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) and Österreichischer Rundfunk.*

54 In particular, Article 13. *Rundfunk*, § 67.

55 *Ibid*., § 70.

56 *Ibid*., § 72.

57 *Ibid*., § 84.

58 *Ibid*., § 88.

59 Judgement of the Court, 6 November 2003, Case C-101/01, *Bodil Lindqvist*.

60 *Ibid*., § 13.

61 *Ibid*., § 72.

62 *Ibid*., § 79.

between the rights and interests involved.[63] It is the responsibility of national authorities and courts, the Court emphasised, to ensure a fair balance between the rights and interests possibly affected by the implementation of EU data protection law.[64]

The *Satamedia* case concerned the interpretation of Directive 95/46/EC[65] in relation to proceedings where what was at stake, according to the EU Court of Justice, was the need to reconcile «*the protection of privacy and freedom of expression*».[66] In its 2008 judgement for the case, the Court insisted on the idea that the obligation to reconcile both rights lies on Member States.[67] In relation to this reconciliation, it just noted that the protection of the fundamental right to privacy requires that any derogations and limitations to EU data protection law must apply only insofar as it is strictly necessary.[68]

3.1.2. Invalidity of EU law due to no insurance of fair balance

The *Schecke* case diverged from the previously mentioned cases because it was not (primarily) a reference for a preliminary ruling on the interpretation of Directive 95/46/CE,[69] but on other EU provisions. The EU Court of Justice, after mobilizing both the Charter and the Strasbourg case law, eventually declared some of the contested provisions partially invalid on the grounds that the EU legislator had not ensured a fair balance between the EU's interest «*in guaranteeing the transparency of its acts and ensuring the best use of public funds against the interference with the right of the beneficiaries concerned to respect for their private life in general and to the protection of their personal data in particular*»,[70] in relation to the data of natural persons.[71]

3.2. Balancing intellectual property against data protection (as a right)

In the *Scarlet* and *Netlog* judgements, the Court of Justice followed in part its case law derived from the 2008 *Promusicae* decision. In that ruling, the Luxembourg Court had to provide guidance on the relation between copyright enforcement and the protection on personal data; more concretely, on the interpretation of EU law regarding the possible obligation of Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings.[72] The Court

63 *Ibid.*, § 85.

64 *Ibid.*, § 90.

65 *Ibid.*, § 1.

66 *Ibid.*, § 54.

67 Idem.

68 *Satamedia*, § 56.

69 Although it was so subsidiarily.

70 *Schecke*, § 77.

71 *Ibid.*, § 89.

72 *Promusicae*, § 41.

of Justice's answer to the referring court was that Member States must take care to allow a fair balance to be struck between the various fundamental rights protected by the EU legal order both when transposing EU law and when implementing transposing measures:[73] mechanisms allowing for different rights and interests to be balanced are contained in EU law and in national law transposing it,[74] but, in addition, when implementing the measures transposing EU law, national authorities and courts must interpret such measures in a manner ensuring that the interpretation is not in conflict with any fundamental principles or general principles of EU law, including the principle of proportionality.[75]

3.2.1. The right to personal data protection as the applicable right

A first key difference between *Promusicae* and *Scarlet* and *Netlog* is that, in the latter, the EU Court of Justice singled out as one of the applicable fundamental rights the right to the protection of personal data, whereas in *Promusicae* it didn't, mentioning instead, for the purpose of the balance to be struck with the right to intellectual property, the right to respect for private life.

In the *Scarlet* and *Netlog* cases, the referring courts had not mentioned at all the EU fundamental right to personal data protection, or even the Charter, alluding instead to the ECHR – and in particular to Article 8 of the ECHR on the right to respect for private life. The EU Court of Justice nevertheless took the deliberate decision to reformulate their questions as inquiries into the interpretation of EU law «*read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights*»,[76] amongst which it identified the right to the protection of personal data.

In doing so, the Court adhered partially to the advice of Advocate General Cruz Villalón expressed in his Opinion for *Scarlet*.[77] Noting that since the entry into force of the Lisbon Treaty the rights established by the ECHR are still applicable as general principles of EU law,[78] but that the Charter has now acquired binding force, the Advocate General had argued that recourse to the former shall not be necessary anymore insofar the rights it safeguards are covered by the latter.[79] Observing also that Article 52(3) of the Charter establishes that the Charter's rights corresponding to ECHR rights are to be interpreted in the

73 *Ibid*., § 70.

74 *Ibid*., § 66. This idea is taken from *Lindqvist* (§ 82), where, as a matter of fact, it referred to the conciliation in Directive 95/46/EC of the safeguard of fundamental rights and the insurance of the free movement of data.

75 *Promusicae*, § 68 (with a reference to Lindqvist, § 87, and to Judgement of the Court (Grand Chamber) of 26 June 2007, Case C-305/05, *Ordre des barreaux francophones et germanophone and Others v Conseil des ministres*, § 2).

76 *Scarlet*, § 29 and Netlog, § 26.

77 Opinion of Mr Advocate General Cruz Villalón delivered on 14 April 2011 in Case C-70/10.

78 *Ibid*., § 29.

79 Idem.

same light, he had advanced that, at least in the circumstances of the case, Article 8 of the ECHR corresponded to two Charter's provisions: Article 7, on the right to respect to private life, and Article 8, on the protection of personal data.[80] In addition, he pointed out, Article 52(1) of the Charter, which specifies the conditions in which the Charter's rights can be limited, also corresponds, to some degree at least, to the content of Article 8 of the ECHR, although this provision does not refer to any «*limitations*», but to «*interferences*».[81] All in all, Cruz Villalón suggested that the mention of Article 8 of the ECHR by the referring court be reformulated and replaced with a reference to Articles 7, 8 and 52(1) of the Charter, to be interpreted, nonetheless, to the necessary extent, in the light of Article 8 of the ECHR.[82] The Court of Justice integrated this suggestion only to a point. It granted precedence to the Charter over the ECHR, but cited exclusively one Charter provision in relation to the protection of personal data: Article 8.

3.2.2. A strong even if laconic assertion of the lack of fair balance

A second significant difference between *Promusicae*, and *Scarlet* and *Netlog* concerns the balancing exercise between conflicting rights. *Promusicae* could be regarded as an example of the EU Court of Justice's tendency to defer balancing operations related to the application of EU data protection law to national authorities and courts, although providing them some orientation on how to do such balancing. In contrast, in *Scarlet* and *Netlog* the Court did not merely highlight that national authorities and courts must strike a fair balance between the involved rights, but took a clear position in relation to the lack of fair balance struck between the fundamental rights conflicting in the main proceedings.

A further extraordinary step taken by the Luxembourg Court in *Scarlet* and *Netlog* refers to the straightforwardness of the balancing exercise applied. In his Opinion for *Scarlet*, Advocate General Cruz Villalón had explored lengthily whether the monitoring system at stake could be regarded as a permissible «*limitation*» of the rights recognised by the Charter, in the sense of its Article 52(1), or as an «*interference*» with Article 8(1) in the sense of Article 8(2) of the ECHR.[83] He had expressed that it was difficult to evaluate the specific impact of the monitoring system on the right to the protection of personal data,[84] *inter alia* because of the difficulties related to determining whether IP addresses constitute personal data,[85] but that, in any case, the system could certainly potentially affect the right to the protection of personal data sufficiently as to allow its qualification as «*limitation*» in the sense of Article

80 *Ibid.*, § 31.

81 *Ibid.*, § 32.

82 *Ibid.*, § 43.

83 *Ibid.*, § 72.

84 *Ibid.*, § 74.

85 *Ibid.*, § 75.

52(1) of the Charter.[86] Having said so, he noted the same provision allows limitations under certain conditions,[87] in particular if they are necessary to protect the rights and freedoms of others.[88] Limitations must notably be «*provided by law*», an expression that in his view had to be interpreted in the light of Strasbourg's case law on the requirement of «*in accordance with the law*» of Article 8(2) of the ECHR, which eventually led him to conclude that the imposition of the monitoring system did not comply with such requirement.[89]

The Court of Justice passed over all these considerations. It simply proclaimed that the measures at stake implied the systematic processing of personal data and, on these grounds, concluded that the right to data protection had been affected, and that no fair balance had been struck with the right to intellectual property. It did not explain how did exactly the processing in question constitute a «*limitation*» of the right, or why could it not be regarded as a legitimate limitation, if it was a «*limitation*». This approach can be seen as contrasting with its general case law on the need to articulate any balance between fundamental rights in a rigorous manner respectful of the principle of proportionality, as well as with its numerous previous efforts emphasising the relevance of the Strasbourg case law and (more recently) the provisions of the Charter for the realisation of a rigorous and *fair* balance.

4. CONCLUDING REMARKS

To recapitulate, the Luxembourg's Court case law on the protection of personal data is marked by contradictory approaches as to which are the relevant fundamental rights applicable for the interpretation of EU law. When dealing directly with Directive 95/46/EC, the Court tends to read this instrument in the light of the right to respect for private life as safeguarded by Article 8 of the ECHR. When it interprets Directive 2002/58/EC, which is supposed to develop Directive 95/46/EC, but, for chronological reasons, bears an explicit mention of Article 8 of the Charter, the Court refers more easily to the existence, and applicability, of a EU fundamental right to the protection of personal data. From *Rundfunk* to *Promusicae*, the Court had been extremely cautious with regard to determining the scope of EU personal data protection law and weighing up conflicting fundamental rights.[90] When dealing directly with the interpretation of Directive 95/46/EC, it has generally left the balancing between any rights and interests at stake in the hands of domestic courts and authorities.[91]

86 *Ibid*., § 80.

87 *Ibid*., § 87.

88 *Ibid*., § 92.

89 *Ibid*., § 108.

90 Opinion of Advocate General Kokott for Case C-73/07, § 46.

91 A tendency that has been criticised. See, for instance: Spiecker Döhmann, I. and M. Eisenbarth (2011). Kommt das ,,Volkszählungsurteil» nun durch den EuGH? - Der Europäische Datenschutz nach Inkrafttreten des Vertrags von Lissabon. *Juristenzeitung*, 4(2011), p. 175.

Against this heterogeneous background, the *Scarlet* and *Netlog* judgements stand out as peculiar. Not only do they assert the existence of a EU right to data protection and its precedence over the application of Article 8 of the ECHR for the interpretation of EU law insofar as the protection of personal data is concerned, but they have also lead to a sound affirmation of the incompatibility with EU fundamental rights standards of the imposition of the systematic monitoring of communications in the name of copyright enforcement.

These developments might mark the beginning of new attitude towards the balancing of conflicting fundamental rights by the Luxembourg Court. They might also, however, just continue to feed the diversity of the Court of Justice's approaches towards data protection, a diversity of views (or mere confusion?) that will probably persist as long as the Court refuses to openly acknowledge that the catalogue of EU fundamental rights includes nowadays a right to the protection of personal data. The legislative proposal introduced in January 2012 by the European Commission to replace Directive 95/46/EC with a new Regulation[92] straightforwardly asserts the existence of such a right,[93] even if, despite including provisions on its reconciliation with other interests and rights, such as the right to freedom of expression, it lacks any specific mechanism for its reconciliation with copyright enforcement[94] - confirming (if necessary) the importance of the Court's role in drawing up the right's shape, and in clarifying how to deal with its balancing.

5. BIBLIOGRAPHY

Arenas Ramiro, M. (2006). *El derecho fundamental a la protección de datos personales en Europa*. Valencia: Tirant Lo Blanch.

Bobek, M. (2011). Joined Cases C-92 & C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert*, Judgement of the Court of Justice (Grand Chamber) of 9 November 2010, nyr. *Common Market Law Review,* 48, 2005-2022.

Coudray, L. (2010). *La protection des données personnelles dans l'Union européenne: Naissance et consécration d'un droit fondamental*. Berlin: Éditions universitaires européennes.

De Hert, P. and S. Gutwirth (2009). Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action. In Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile De Terwangne & Sjaak Nouwt (eds.), *Reinventing Data Protection?* (pp. 3-44). Dordrecht: Springer.

92 European Commission (2012). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25.1.2012, Brussels.

93 *Ibid*., notably pp. 2, 3, 6, 15 and 40.

94 The protection of intellectual property is alluded as potentially affected by the proposal (*ibidem*, p. 7), a conflict developed only in relation with the protection of the copyright of profiling software (*ibidem*, p. 25).

Docquir, B. (2009). Arrêt *Satamedia*: la (re)diffusion d'informations publiques dans les médias et les exigences de la protection des données. *Revue européenne de droit à la consommation,* 2-3, 560-581.

European Commission (2012). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation*)*, COM(2012) 11 final, 25.1.2012, Brussels.

González Fuster, G. and R. Gellert (2012). The fundamental right of data protection in the European Union: in search of an uncharted right. *International Review of Law, Computers & Technology, 26*(1), 73-82.

González Gozalo, Alfonso (2008). El conflicto entre la propiedad intelectual y el derecho a la portección de datos de carácter personal en las redes *peer to peer*. *Pe. i: Revista de propiedad intelectual*, 28, 13-68.

González Vaqué, L. (2008). El TJCE se pronuncia sobre la obligación de comunicar datos personales a fin de garantizar la protección de los derechos de autor en un procedimiento civil: la sentencia «Promusicae». *Aranzadi Unión Europea, año 34, mayo*(5), 5-14.

Groussot, X. (2008). Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, Judgement of the Court (Grand Chamber) of 28 January 2008: Rock the KaZaA: Another Clash of Fundamental Rights. Common Market Law Review, 45, 1745-1766.

Hins, W. (2010). Case C-73/07, Tietosuojavaltuutettu v. Stakunnan Markkinapörssi Oy and Satamedia Oy, judgment of the Grand Chamber of 16 December 2008, not yet reported. Common Market Law Review, 47, 215-233.

Oliver, P. (2009). The protection of privacy in the economic sphere before the European Court of Justice. Common Market Law Review, 46, 1443-1483.

Ordóñez Solís, D. (2011). Las descargas ilegales en Internet: el contexto jurídico europeo de la Ley Sinde. Unión Europea Aranzadi, año 2011 - noviembre(11), 7-20.

Piñar Mañas, J. L. (2003). El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas. *Cuadernos de Derecho Público, 19-20*(mayo-diciembre), 44-90.

Ruiz Miguel, C. (2003). El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Unión Europea: Análisis crítico. *Revista de Derecho Comunitario Europeo, 7*(14), 7-43.

Siemen, B. (2006). *Datenschutz als europäisches Grundrecht*. Berlin: Duncker & Humblot.

Spiecker Döhmann, I. and M. Eisenbarth (2011). Kommt das ,,Volkszählungsurteil» nun durch den EuGH? - Der Europäische Datenschutz nach Inkrafttreten des Vertrags von Lissabon. *Juristenzeitung, 4*(2011), 169-177.

THE EMERGING RIGHT TO BE FORGOTTEN IN DATA PROTECTION LAW: SOME CONCEPTUAL AND LEGAL PROBLEMS

David Lindsay[1]
Associate Professor, Faculty of Law, Monash University, Melbourne, Australia

ABSTRACT: The proliferation of ubiquitous, personal digital traces in networked environments poses fundamental challenges for identity-formation, privacy and autonomy in contemporary societies. While these traces may be shared in one context, their persistence and accessibility mean that they may be accessed and used to form judgments in an entirely different context, causing tangible harms to data subjects. Moreover, the ubiquity and accessibility of personal data generated by private individuals has the potential to erode autonomy and self-determination, which are already under threat in contemporary 'liquid' societies. Concerns about the uncontrolled circulation of personal data have given rise to proposals for introducing a 'right to be forgotten', including the current proposal from the European Commission to introduce such a right, as part of a fundamental reform of the European data protection framework. This paper supports the European proposal, arguing that a rights-based data protection framework is the best mechanism for appropriately balancing the right to privacy with countervailing rights and interests, especially the right to freedom of expression. The paper concludes by identifying two fundamental legal issues in the application of the proposed new right to social networking services (SNS) that seem likely to pose ongoing challenges to data protection laws: the extent to which the use of SNS by private individuals should be exempted from regulation as personal and private use, and the extent to which private individuals should be regulated as data controllers.

KEYWORDS: Privacy, social networking services, data protection, delete, identity, liquid modernity.

1. INTRODUCTION

The popularity of social networking services (SNS) gives rise to complex questions about the relationship between self, identities and privacy. As inter-personal relationships migrate to digital networks, personal information that is shared persists over time and may be highly accessible. When personal information that is shared in one context is later accessed and used in another context, this may cause tangible harms to the individual concerned, as judgments are made based on de-contextualised, outdated, partial or inaccurate information. Moreover, the increasing accessibility of personal information about individuals poses threats to self-determination and autonomy, as people face the threat of becoming imprisoned by their digital pasts.

1 The author would like to thank an anonymous reviewer for helpful comments on a draft of this paper.

These concerns have given rise to proposals for giving individuals greater control over the management of their digital data. One response has been to introduce legal rights for individuals to, in certain circumstances, delete or erase information about themselves, which has become commonly known as the 'right to be forgotten'. Largely in response to concerns about the uncontrolled circulation of personal information by means of new technologies and services, such as SNS, in early 2012 the European Commission incorporated a version of a right to be forgotten in its proposed new data protection instrument.

This paper introduces and analyses some conceptual and legal issues involved with the proposed right to be forgotten. First, it explores the social and policy challenges posed by the ubiquity of persistent and highly accessible digital personal information, especially in the context of SNS. In doing so, the paper examines some of the complexities associated with identity-formation, privacy and autonomy in contemporary societies, drawing from the work of the prominent sociologist, Zygmunt Bauman. Secondly, it outlines the justification for introducing a right to be forgotten, including why a legal right is superior to technology-based solutions, and why it is appropriate for the right to be formulated within the framework of data protection laws. Thirdly, the paper explains the background to the right to be forgotten in data protection law and policy, outlining early proposals to provide for the deletion of personal information in data protection instruments, and analysing the extent to which the 1995 European Data Protection Directive ('DPD')[2] implements deletion rights. Fourthly, it introduces and explains the version of the right to be forgotten incorporated in the proposed new European data protection instrument, including an explanation of how the proposed right goes beyond the protections conferred by the DPD, a critical analysis of the exceptions to the proposed right, and an assessment of ambiguities and uncertainties in implementing the proposed right.

2. SOME PARADOXES OF PRIVACY AND DIGITAL IDENTITY

This section of the paper explores the difficulties and complexities that arise from the proliferation of personal digital traces in networked environments. In doing so, it explains some of the concerns in the privacy literature that a lack of individual control over personal information may erode autonomy and self-determination, and undermine the ability to form inter-personal relations. Drawing largely from the work of Zygmunt Bauman, the section then explains and analyses some of the paradoxes of identity-formation in contemporary, 'liquid' societies, which lead to imperatives to establishing identities by revealing personal information that inevitably corrode a sense of autonomy and self-determination, as that information is used against the individual.

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* [1995] OJ L281/31. ('DPD').

2.1. The problem of digital traces

In contemporary societies people leave behind ever-growing digital traces.[3] Our digital traces give rise to considerable personal and social difficulties. These complexities are associated with the following default features of networked digital data:

- *Persistence* – once digital data has been generated, it is generally durable over time;
- *Replicability* – digital data is easily replicated, so that removing the original source of the data does not remove copies of the data; and
- *Searchability* - which allows the ready identification of much relevant information in response to relatively unsophisticated strategies.

The default features of networked data illustrate the in-built biases of our information infrastructure towards permanence and accessibility. Yet information in networked digital form –durable, replicable and searchable– is thoroughly decontextualised. While computer memory is superior to human memory in terms of permanence and comprehensiveness, it is humans who ultimately give information meaning and depth, by applying context to data.[4]

The problems with our persistent digital traces essentially arise from the extent to which information posted in one context may be accessed and used in different contexts.[5] The most commonly-cited examples involve information about the private lives of people that is later used by others in professional or employment contexts. The case study, commonly presented as an object lesson, is the story of Stacy Snyder, an American university student, who posted a photograph of herself in a pirate's hat and drinking from a plastic cup to her MySpace page, which later led to her university refusing to allow her to graduate.[6] But people may be legitimately concerned about their digital traces even if the consequences are confined to embarrassment or humiliation. For example, Jessica Ewing, a Google search engineer, reportedly once requested the Google search team to alter the first search result for her name, which returned an 'embarrassing' photograph of her as a 13-year-old mathlete.[7]

In addition to the misuse of decontextualised information, information returned in response to a search may be incomplete. For example, the plastic surgeon, Hugo Russo, one of 90 Spanish citizens to complain to Spain's Data Protection Agency (AEPD) about Google search returns, was concerned that results for his name invariably returned hits for a twenty-year-old malpractice suit, without any mention of a subsequent acquittal.[8] The

3 See Koops (2011), distinguishing between digital footprints and data shadows: at 230.

4 See boyd (2010); Mayer-Schönberger (2009).

5 On the importance of context and the risks of de-contextualisation see: Nissenbaum (2004); Dumortier (2009).

6 Mayer-Schönberger (2009), 1-2; Rosen (2010) 32.

7 Levy (2011) 174.

8 An order by the Spanish Data Protection Agency for Google to remove links has been appealed to a Spanish Court: *Google Spain and Google Inc v Agencia Española de Protección de Datos* (Audiencia

picture that emerges is one of irrelevant or partial information being persistently used in inappropriate contexts and resulting in tangible harms. Moreover, the operation of search engine algorithms, such as Google's PageRank, often results in the most embarrassing or humiliating information about a person dominating search returns.[9] This can disturb even Google executives, such as Susan Wojcicki, who was alarmed to discover that the second return from a Google search was a blog posting that falsely accused her of taking credit for developing AdSense.[10]

2.2. Digital traces, freedom and self-development

Apart from the harms that result when decontextualised or fragmented information is inappropriately used, there are more fundamental concerns that are related to the tradition in privacy theory that links privacy rights with self-development. Rachels (1975), for example, claimed that, over and above specific harms, rights to privacy are needed to allow people to maintain different relationships with different people, or with groups of people. For instance, while it might be perfectly acceptable to share some personal information with close friends, it may be inappropriate to reveal the same information to business associates. According to Rachels, therefore, privacy is an aspect of self-development in that it provides the pre-conditions for establishing and maintaining relationships of differing degrees of richness with different people.[11]

This view corresponds with the more general notion that an ability to control information about ourselves and, concomitantly, to control who has access to certain information about us, are pre-requisites for autonomous decision-making. The classic illustration of the way in which autonomy is deprived is what Goffman (1961) referred to as 'total institutions', meaning an institution, such as a prison or asylum, in which the inmates are fully documented and subject to bureaucratic rules. In his landmark study, Goffman showed how this leads to the undermining of identity, and is associated with demoralisation, de-skilling and the erosion of autonomy.

Our digital traces therefore have the potential to act as a virtual prison, to keep us tethered to expressions of ourselves that are outdated, incomplete or inaccurate. Consequently, by providing de-contextualised access to previously inaccessible personal information, our digital traces may undermine autonomous decision-making and promote social conformity.

Nacional, Madrid). The Spanish court (the Audiencia Nacional) has, in turn, referred one of the cases, involving an outdated foreclosure notice, to the European Court of Justice for a ruling on nine key questions: Peguera (2012).

9 On the operation of PageRank, and its inherent biases, see Levy (2011) 21-24; Vaidhyanathan (2011) 60-64.

10 Levy (2011) 174.

11 But see the criticism of Rachels in Reiman (1976).

2.3. Digital traces, Bauman and the paradoxes of identity formation

The view that privacy, or the ability to selectively withhold and reveal personal information,[12] is a necessary pre-condition for individual self-development is built on fundamentally liberal conceptions of the individual as autonomous decision-maker. In fragmented, post-modern societies, however, the liberal model, based upon a fixed individual linearly developing his or her capacities over time, is difficult to sustain. Problems of self, identity and privacy in contemporary societies are more complex than the liberal narrative of individual emancipation suggests.

The sociologist, Zygmunt Bauman, is one of the most prominent analysts of problems of identity in post-modern or, in his terms, 'liquid' societies. According to Bauman, an important distinction can be drawn between solid modernity, in which individual identity is anchored by reference to the certainties of birth, gender and nationality, and liquid modernity, in which identity is fragmented, discontinuous and ambivalent. Instead of a solid individual identity as a pre-condition for autonomous decision-making, liquid modernity is characterised by deep anxiety about identity, leading to obsessive re-invention (or consumption) of identities. Consequently, instead of the focus being on an individual's struggle to build an identity emancipated from tradition and conformism, there is a continual, anxiety-induced search for identity, which can never quite be achieved. This leads Bauman to famously conclude that, in liquid societies, individualisation is 'a fate and not a choice'.[13]

As Přibáň has explained, the imperative for perpetual identity creation leads to 'a growing gap between the individual as a self-asserted and self-created member of modern society and the individual as a member of society assigned to act individually without ever having any choice than to act in the prescribed way'.[14] This is clearly related to paradoxes of identity formation through social networking. Bauman regards the relatively ephemeral bonds of online communities, which allow for perpetual playing with identity, as a response to the social imperatives for fluid identities.[15] Yet, once social interactions have been recorded in a permanent form, then the online identities that have been created can result in the very inflexibility of identity that is derided by a society that celebrates continual re-invention.

Although Bauman does not expressly make this point, our societies are neither fully liquid nor fully solid, but are stranded between; while there are demands for adaptability and flexibility, there are countervailing demands from institutions and employers for certainty and continuity. The key paradox is that the liberation promised by online identity exploration can limit the ability to re-make oneself.

12 See Nagel (1998).

13 Bauman (2000) 34.

14 Přibáň (2007) 7.

15 See Bauman (2004); Bauman (2011).

3. THE CASE FOR A LEGAL RIGHT TO BE FORGOTTEN

The public sphere, or what boyd refers to as 'networked publics',[16] has been swamped by private and personal information. Some, and especially those with a commercial interest in people sharing personal information, have suggested that social norms will adapt, and society will become more tolerant of individual failings and foibles. For example, Mark Zuckerberg famously said:

> … people have gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.[17]

Yet, as peoples' private lives have progressively bled into the public, there are no indications either that social attitudes towards what is private and what is public are changing, or that society is becoming more tolerant. Indeed, as Nagel (1998) pointed out more than a decade ago, the increased revelation of personal information seems matched, if anything, by greater public intolerance of 'deviant' behaviour.

People therefore seem caught between the worst of all worlds: revealing information to create and reinforce evanescent and fragmented identities, which can then be used to form judgments based on the assumption that the information conveys insights about a core identity. The extent to which people are concerned about judgments that may be formed about them based on publicly available private information is seen in the growth of private reputation management services, such as reputation.com,[18] and even non-profit reputation sanitising sites, such as the Web 2.0 suicide machine.[19]

Once we accept that, in 'fluid' societies, people feel compelled to reveal personal information about themselves, and that this information will be used by others, including those with a degree of power, to form judgments, then there is a need to restore a degree of control over this information. Apart from the 'hit-or-miss' strategy of market-based services, prominent proposals have suggested introducing technological constraints on digital persistence and replicability, such as Mayer- Schönberger's proposal for setting expiration dates for digital data.[20] There are, however, a number of problems with relying solely on technology-based solutions. First, these approaches appear to assume that current technological defaults are the source of the problem rather than a symptom of deeper social processes. Secondly, if the onus is placed on users to set expiry dates, this may be regarded as too onerous, and ignored by most people. Thirdly, it would be difficult to persuade technology companies, who have commercial interests in the generation of open access data, to change current technological defaults. Fourthly, any technology-based solution is

16 See boyd (2010).

17 Johnson (2010).

18 See <www.reputation.com>, Retrieved 19 March 2012; Bartow (2009).

19 See <suicidemachine.org>, Retrieved 19 March 2012.

20 Mayer-Schönberger (2009), 169-195.

subject to counter-technologies, which can be designed to circumvent privacy-protective technologies.

Concerns about the extent to which access to, and use of, personal information may undermine identity-formation and individual autonomy fall squarely within legal responses that recognise privacy as a fundamental right. Moreover, given that data protection laws can be seen as a reaction to the ubiquitous production and circulation of personal information by governments and private enterprise,[21] it seems reasonable to assume that the data protection framework can be adapted to apply to the ubiquitous production and circulation of personal information, such as in the context of Web 2.0 applications. In addition, an individual right to delete personal information can build on existing data protection principles which, as explained below, have a long tradition of countenancing the erasure of personal data. Finally, a rights-based framework for addressing the problems of digital traces can establish appropriate mechanisms for balancing individual rights to privacy and other rights and interests, and especially the right to freedom of expression. In this respect, appropriately balancing rights to data autonomy, on the one hand, and freedom of expression, on the other, are both too complex and important to be left to the private sector.

4. BACKGROUND TO THE RIGHT TO BE FORGOTTEN IN DATA PROTECTION LAW

This section of the paper introduces the current proposals for adopting a right to be forgotten within the European data protection framework. It then explains the history of proposals for introducing a principle requiring data controllers to erase personal data when it is no longer needed, which the paper refers to as the 'deletion principle'. Finally, the section analyses the extent to which the deletion principle is embodied in the 1995 DPD, which forms the current baseline for the regulation of the processing of personal data in the European Union.

4.1. EU Data Protection Reform and the Right to be Forgotten

In January 2012, the European Commission released proposals for a new EU framework for data protection designed to replace the existing data protection regime, which is based on the DPD. The proposed new framework includes a General Data Protection Regulation ('GDPR'),[22] a key component of which is a distinct, express right to be forgotten.

The background to the GDPR makes it clear that the right to be forgotten is, in particular, designed to address the increased collection and disclosure of personal data by new technologies and services, and especially by SNS. The current EU reform process commenced

21 Ibid. 160-161; Simitis (1987) 709-10.

22 European Commission, Proposal for a Regulation of the European Parliament and of the Council *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation). COM(2012) 11 final. Brussels: 25 January 2012.

in 2009, with specific proposals being formulated in a Communication from the European Commission issued in November 2010.[23] The Communication referred to existing access and rectification rights, but went on to point out how exercising these rights were particularly challenging in the online environment, adding that:

> The example of online social networking is particularly relevant here, as it presents significant challenges to the individual's effective control over his/her personal data.[24]

The Communication went on to indicate that, in seeking to strengthen individuals' control over their data, it would examine ways of clarifying the right to be forgotten, which it defined as 'the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes'.[25]

4.2. A concise history of the deletion principle

Proposals for imposing obligations to erase personal data have been made from the earliest stages in the development of data protection laws. Data protection principles can effectively be traced to the 1973 report of an Advisory Committee of the US Department of Health, Education and Welfare ('HEW Report').[26] The HEW Report first formulated a code of practice, known as the fair information practices (FIPs), to apply to the collection, storage, use and dissemination of personal information. While the deletion principle was not part of the FIPs, the report included proposed general safeguards to apply to automated data processing, which included the specific requirement to '(e)liminate data from computer-accessible files when the data are no longer timely'.[27]

The concerns expressed in the HEW Report did not, however, lead to the wholesale adoption of the deletion principle. While the report did result in the *Privacy Act of 1974,* 5 USC §552(a) (2006), which applied the FIPs to federal government agencies, the Act incorporated access and correction rights, but no effective rights to require the erasure of data.

Meanwhile, at the international level, the antecedents of data protection principles are found in two instruments developed in the mid-1980s: the Council of Europe's *Convention on Data Protection* (the 'CoE Convention')[28] and the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (the 'OECD Guidelines').[29] During the pro-

---

23 European Commission (2010).

24 Ibid. 7.

25 Ibid. 8.

26 Secretary's Advisory Committee on Automated Personal Data Systems (1973).

27 Ibid.

28 Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* adopted by the Council of Europe Committee of Ministers on 28 January 1981.

29 Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Data,* adopted by the OECD Council on 23 September 1980. ('OECD Guidelines').

cess of developing both instruments, concerns were expressed about the potential problems created by relatively permanent storage of personal data. These concerns were expressed quite early in the processes of developing the two instruments. For example, an Annex to a Resolution adopted by the Council of Europe in 1973 provided that:

> Rules should be laid down to specify periods beyond which certain categories of information should no longer be kept or used.[30]

The Explanatory Report to the Resolution further suggested that the proposed rules could be implemented by computers being programmed to erase data after a specified terminal date. Similarly, an early draft of the OECD Guidelines, which adopted a version of the FIPs, included a time limitation principle, which provided that:

> Personal data in a form that permits identification of the data subject should, once their purposes have expired, be destroyed, archived, or deidentified.[31]

Despite the attention given to the issue, proposals to introduce a deletion principle were not fully implemented in express obligations to erase data. As Michael Kirby explained, the OECD Expert Group decided to omit the time limitation principle on the basis that the security safeguards and use limitations principles provided sufficient protection, 'without imposing an expensive and possibly privacy-harmful obligation of culling and destroying personal information'.[32] The deletion principle is therefore not included as a principle in the OECD Guidelines, with the sole reference being confined to the following highly qualified statement in the Explanatory Memorandum, in relation to the purpose specification principle:

> ... when data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed (erased) or given an anonymous form.[33]

The CoE Convention went further than the OECD Guidelines, with Article 5, the data quality principle, providing that personal data should be 'preserved in a form which permits the identification of the data subjects for no longer than is required for the purpose for which those data are stored'. This is supported by Article 8(c), which provides a right to obtain rectification *or erasure* of data where these have been processed contrary to laws implementing the data quality principle. These provisions, however, while envisioning the possibility of erasure, fall short of a fully-fledged deletion principle. Moreover, as suggested by Warner, the subsequent development of data protection law in Europe tended to subsume any rights in the destruction of personal data within the use minimisation principle, thereby

30 Council of Europe, Committee of Ministers, *Resolution (73) 22 On the Protection of the Privacy of Individuals Vis-à-vis Electronic Data Banks in the Private Sector,* Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies, Annex, 4.

31 Kirby (1980) 58.

32 Ibid. 58-9.

33 OECD Guidelines, Explanatory Memorandum, paragraph [54].

focusing attention on controlling the uses to which personal data might be put rather than on the continued existence of the data.[34]

4.3. The 1995 Data Protection Directive

In commenting on the EU data protection reform program, Viviane Reding, the EU Commissioner for Justice, Fundamental Rights and Citizenship, referred to proposals for 'strengthening' the right to be forgotten.[35] As Koops points out, this implies that such a right already exists, at least to some degree, under current EU data protection law.[36]

The DPD is the most comprehensive data protection law to date,[37] being aptly described as 'the high-water mark of substantive legal protection of information privacy'.[38] As such, it provides a good baseline for assessing the extent to which current data protection laws implement the deletion principle.

The DPD adopts a 'holistic' approach to data protection regulation, applying minimum principles to all stages of data processing, and generally not distinguishing between collection, storage, use or disclosure. In this respect, it applies the fundamental principle that data processing is permissible only in certain enumerated circumstances, such as that the data subject has given unambiguous consent, processing is necessary for performance of a contract to which the data subject is a party, or processing is necessary for compliance with a legal obligation of the data controller.[39]

The DPD provides for the erasure of personal data in three distinct provisions. First, Article 6(1) requires Member States to include an obligation for personal data to be:

> kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.[40]

While this obligation can be complied with by the deletion of data, it falls short of the deletion principle as compliance may also be achieved by anonymisation, and as it imposes an obligation on data controllers, but fails to confer corresponding rights on data subjects.

Secondly, Article 12, which provides for access and correction rights, requires Member States to give data subjects the right to obtain:

---

34 Warner (2005) 86.

35 Reding (2011) 4.

36 Koops (2011) 232-3.

37 Bygrave (2002) 30.

38 Cate (2006) 351.

39 DPD, Article 7.

40 DPD, Article 6(1)(e).

> … as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of … [the DPD], in particular because of the incomplete or inaccurate nature of the data.[41]

Although this appears to give a right to apply for erasure of data, it is subject to two important qualifications. First, the right arises only where processing is contrary to the provisions of the DPD. Secondly, it is possible to interpret the clause beginning with 'in particular' as limiting the right to circumstances where the data are incomplete or inaccurate.[42] In the absence of more specific guidance, the extent to which Article 12 incorporates the deletion principle remains a matter for national implementation.

Thirdly, Article 14 of the DPD requires Member States to confer on a data subject the right:

> … to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation.

As with the other two relevant articles of the DPD, the extent to which the right to object incorporates the deletion principle is highly qualified. First, it is confined to where processing is permitted as being necessary in the public interest, or for the legitimate interests of the data controller or another person. Secondly, the provision places the onus on the data subject to establish that there are 'compelling legitimate grounds' to object to the data processing. Thirdly, it gives national legislatures a broad discretion to carve out exceptions to the right to object. Finally, by not specifically referring to erasure, it creates the possibility that the objection may be justified for some forms of processing, such as use or disclosure, but not other forms, such as storage.[43]

An analysis of the specific provisions of the DPD which deal with the possibility of erasure therefore indicates that, although it goes beyond previous data protection instruments in creating the possibility for personal data to be erased in certain circumstances, the degree to which it implements the deletion principle is limited. This suggests that, as with prior data protection instruments, such as the OECD Guidelines and CoE Convention, concerns with the potential negative consequences of data retention were, to an extent, outweighed by concerns that retaining the information might be beneficial to data subjects and concerns about the costs that an obligation to delete data might impose on public and private sector data controllers. The proliferation of personal data generated by individuals in the context of Web 2.0 applications, however, alters this calculus, as it is much less likely that the relatively trivial information published on applications such as SNS will have long-term benefits for data subjects. Nevertheless, as is explained below, the provisions of the DPD analysed in this section of the paper form the basis for a stronger form of the deletion principle in the GDPR.

---

41 DPD, Article 12(b).

42 See Koops (2011).

43 Ibid. 240.

5. THE RIGHT TO BE FORGOTTEN IN THE PROPOSED GDPR

This section of the paper analyses the extent to which the proposed GDPR implements the deletion principle. First, it introduces the general framework for the regulation of the processing of personal data under the GDPR. Secondly, it explains the adoption of a right to be forgotten in Article 17 of the GDPR and examines how the proposal extends the rights of data subjects beyond those conferred by the DPD. Thirdly, it explains how the principle of proportionality is implemented by limitations on, and exceptions to, the right to be forgotten in the proposed GDPR. Finally, it introduces and analyses legal issues that arise in the application of the proposed right to be forgotten to SNS.

5.1. The general framework of the proposed GDPR

The 2010 Communication of the European Commission, referred to above, concluded that a more comprehensive and coherent framework was needed to protect the fundamental right to data protection. As further mentioned, the perceived need for reform was prompted, in part, by threats to the ability of individuals to control their data arising from new technologies and services, such as SNS.[44] From this, it can be inferred that the new framework is intended to extend beyond data processing by public authorities and private companies, and to apply to at least some data processing by private individuals.

Like the DPD, the GDPR generally applies comprehensively to all data processing, and permits data processing only in certain enumerated circumstances which, under Article 6, include that: the data subject has given consent; processing is necessary for the performance of a contract to which the data subject is a party; processing is necessary for compliance with a legal obligation of the data controller; and processing is necessary to protect the vital interests of the data subject.

While this central element of the data protection regime is almost indistinguishable from the analogous provision in the DPD,[45] the proposed GDPR is much more comprehensive and detailed. Two important areas in which this is the case relate to access and correction rights, and rights to object to data processing. An appreciation of the proposed right to be forgotten requires an understanding of how these two areas of the proposed GDPR differ from the analogous provisions of the DPD.

5.2. The right to be forgotten in the proposed GDPR

As explained above, Article 12 of the DPD confers access and correction rights, but erasure rights are limited, and may be confined to where data is incomplete or inaccurate. The proposed GDPR deals with access and correction rights by creating separate rights to rectification, in Article 16, and to be forgotten, in Article 17. The Article 16 right to rectification,

44 See particularly Recital (5) to the proposed GDPR.

45 See DPD, Article 7.

like Article 12 of the DPD, confers a right to obtain rectification where processing does not comply with the data protection regime, and 'in particular because of the incomplete and inaccurate nature of these personal data'. Rather than treating the possibility of erasure within the same provision, however, the proposed GDPR introduces a distinct right to be forgotten in Article 17, which is subject to different limitations to the rectification right.

Article 17(1) of the proposed GDPR, which sets out the right to be forgotten, essentially provides that the data subject has a right to obtain erasure of personal data in the following four circumstances:

- where the data are no longer necessary for the purposes for which they were collected or processed;
- where the legitimacy of the data processing is based on the consent of the data subject and that consent has been withdrawn;
- where a storage period that has been consented to has expired; or
- the processing of the data does not otherwise comply with the GDPR.

These alternative bases for obtaining erasure clearly go beyond the current rights under the DPD by incorporating a stronger form of the data quality principle in Article 6(1)(e) of the DPD, and by specifically providing for deletion where consent is the basis for legitimate processing and that consent has been withdrawn. In addition, Article 17(1) makes it clear that deletion rights are especially relevant where the data subject made the data available when he or she was a child.[46]

As previously explained, Article 14 of the DPD gives data subjects a right to object to the processing of personal data, but this right is highly qualified. The proposed GDPR includes objection rights in Article 19, with Article 19(1) establishing a right to object 'at any time' to the processing of data that is based on:

- protection of the vital interests of the data subject;
- performance of a task carried out in the public interest or the exercise of official authority; or
- the legitimate interests of the data controller.

The proposed objection rights in Article 19(1) deal with each of the limitations on objection rights under the DPD. First, the right to object is extended to where processing is necessary to protect the vital interests of the data subject. Secondly, instead of the data subject bearing the burden of establishing that there are 'compelling legitimate grounds' to object, the onus is placed on the data controller to establish that there are 'compelling legitimate grounds' for the processing which override the fundamental rights and freedoms of the data subject. Thirdly, and significantly, the right to object is specifically related to the right to delete data, in that, where the data subject objects under Article 19, including where there is an objection to the processing of personal data for direct marketing under Article 19(2), this triggers a right to have the data deleted under Article 17.

46 See proposed GDPR, Recital (53).

Under Article 12 of the DPD, where a right of rectification or erasure applies, the data subject has a right to require the data controller to notify any third parties to whom the data have been disclosed of the rectification or erasure 'unless this proves impossible or involves a disproportionate effort'.[47] The extent to which digital information published online may be easily copied and distributed, poses significant challenges for a right to be forgotten. Clearly, the removal of information at one source is meaningless if that information remains otherwise accessible. The proposed GDPR deals with this by imposing greater obligations on data controllers in relation to third party processing. In this respect, Article 17(2) provides that, where a data subject has requested erasure and the data controller has made the personal data public, the data controller must:

> … take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

This clearly goes beyond the current obligation in that it applies automatically where the right to erasure is exercised and it imposes liability for authorising third party publications. There are, nevertheless, obvious uncertainties about what may constitute 'reasonable steps', what may be encompassed by 'technical measures' and what may amount to 'authorising' a publication.

5.3. Limitations on, and exceptions to, the proposed right to be forgotten

Like the DPD, the proposed GDPR is aimed at protecting the fundamental right to protection of personal data. In accordance with the European human rights framework, however, the right is subject to the principle of proportionality, so that limitations are necessary to support other rights and freedoms, especially the right to freedom of expression. Consequently, although the proposed GDPR increases the rights of data subjects, it also incorporates important safeguards for countervailing rights and interests. In relation to the right to be forgotten, these safeguards take the form of exceptions to, and potential derogations from, the proposed right.

Article 17(3) of the GDPR provides that, where the right to be forgotten applies, the data must be erased without delay, unless retention is justified by one of the enumerated exceptions. The exceptions permit the retention of data where this is necessary:

- for exercising the right of freedom of expression as provided for under Article 80 of the GDPR. Article 80 of the GDPR requires Member States to establish derogations to protect the processing of personal data 'carried out solely for journalistic purposes or the purpose of artistic or literary expression';

47 DPD, Article 12(c).

- for protecting the public interest in public health as provided for under Article 81. Article 81 requires the EU or Member States to introduce measures to safeguard the legitimate interests of data subjects in the area of public health;
- for historical, statistical or scientific research purposes in accordance with Article 83. Article 83 essentially provides that personal data may be processed for these purposes only if they cannot be achieved by processing anonymised or de-identified data; and
- for compliance with a legal obligation to retain data under either EU or Member State law.

From the above, it is clearly intended for the permitted exceptions to be highly targeted. For example, the protection of freedom of expression is confined to processing for journalistic purposes or creative expression. Moreover, while, like the similar limitation on the right to object under the DPD, provision is made for Member States to introduce laws overriding the right to be forgotten, unlike the DPD any such laws must comply with criteria that ensure that the laws are not disproportionate.[48]

Apart from the specific exceptions to the right to be forgotten, Article 21 provides for the EU and Member States to restrict the scope of rights and obligations established under the GDPR where it is a necessary and proportionate measure in a democratic society to safeguard specific rights and interests, including public security, crime prevention, revenue protection and investigation of ethical breaches in regulated professions. As the Opinion of the European Data Protection Supervisor (EDPS) on the data reform package points out, there is an apparent overlap between the general derogations permitted under national laws pursuant to Article 21 and the specific exception established under Article 17(3)(d), which allows national laws to override the right to be forgotten provided the laws are in the public interest, respect the essence of the right to protection of personal data and are proportionate to the legitimate aim of the relevant law.[49] Given the potential uncertainty arising from the overlap between Articles 21 and 17(3)(d), there is considerable force in the EDPS recommendation in favour of deleting Article 17(3)(d).[50]

Finally, in certain limited circumstances the data controller may be required to restrict the processing of personal data rather than erasing it.[51] Under Article 17(4), the data may be retained and processed for the following specific purposes: verifying the accuracy of the data where this has been challenged by the data subject; where the controller needs the data for the purposes of proof; where the processing is unlawful and the data subject requests restrictions instead of erasure; and to process the data for the purpose of transmitting it to another service pursuant to the right to data portability.

---

48 Proposed GDPR, Article 17(3)(d).

49 European Data Protection Supervisor (2012) *Opinion of the European Data Protection Supervisor on the data protection reform package,* 7 March 2012: [66]-[67], [149].

50 While there is some ambiguity as to whether the EDPS recommendation is confined to deleting Article 17(3)(d) or favours deleting Article 17(3) as a whole, there is merit in retaining the specific exceptions in Article 17(3)(a)-(c), which specifically refer to Articles 80, 81 and 83.

51 Proposed GDPR, Article 17(3)(e).

5.4. Application of the proposed right to be forgotten to SNS

Although the background to the introduction of a right to be forgotten suggests that it is essentially a response to the significant increase in user-generated content arising from Web 2.0 applications, and especially SNS, there are real questions about the extent to which the proposed GDPR applies to SNS. Apart from jurisdictional issues, there are two main legal issues that arise in applying any data protection framework, including the proposed GDPR, to user-oriented services such as SNS:

1. The application of the regime to data processing for purely personal or domestic purposes, which is dealt with under EU law by what is known as the 'household exemption'; and
2. The extent to which the regime applies to private individuals which, under the proposed GDPR, depends upon whether a person is a 'controller'.

5.4.1. The household exemption

Article 2(2)(d) exempts from the scope of the proposed GDPR data processing:

> by a natural person without any gainful interest in the course of its own exclusively personal or household activity.

An important gloss on the meaning of the terms used in the exemption is provided by Recital (15) to the GDPR, which states that:

> This Regulation should not apply to the processing of personal data by a natural person, which are exclusively personal and domestic, such as correspondence and the holding of addresses, and without any gainful interest and thus without any connection with a professional or commercial activity. The exemption should also not apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.

The difficulties in applying the household exemption to Web 2.0 applications, such as SNS, arises from the extent to which they blur the boundaries between what is public and what is private, as well as what is commercial and what is non-commercial. From Recital (15) it seems that what amounts to a 'gainful interest' may be determined by whether or not there is some connection with a professional or commercial activity. It is also clear from the Recital that the exemption does not apply to those responsible for providing the means for processing data for personal or household activities, meaning that SNS providers are not entitled to the exemption.

Whether or not the exemption applies to individual users of SNS will often come down to whether use of an SNS is an *exclusively* personal or household activity. Some assistance in answering this question may be obtained from the 2009 Opinion of the Article 29 Working Party on online social networking, which addressed the application of the DPD to SNS.[52] In doing so, the Working Party examined whether or not individual SNS users are entitled

52 Article 29 Data Protection Working Party (2009b).

to the household exemption under the DPD, which exempts data processing 'by a natural person in the course of a purely personal or household activity'.[53]

The Working Party concluded that, while the household exemption would generally apply to individual use of an SNS, in certain circumstances the exemption might not apply. First, the Working Party concluded that the exemption would not apply where an individual user acts on behalf of a company or association, or uses the SNS to advance commercial, political or charitable goals. Under the proposed GDPR, it would seem that such users would not be entitled to the exemption as these activities are pursued for 'gainful interest'. Secondly, the Opinion concluded that, where access to profile information extended beyond self-selected 'friends', such as to all members of an SNS, access would extend beyond the personal and domestic sphere, and the exemption would not apply. Thirdly, the Working Party concluded that if users acquired a high number of third party contacts, such as a high number of 'friends', this could be an indication that the household exemption does not apply.

The conclusions of the Working Party that some activities of individual SNS users may not be entitled to the household exemption, and its emphasis on how accessible the information is, find support in the decision of the European Court of Justice in the *Bodil Lindqvist case,*[54] in which the court held that publication of a church newsletter on the Internet, so that the data are accessible to an indefinite number of people, did not fall within the exemption. On the other hand, the drafting history of the GDPR suggests that, in contrast to the Working Party's interpretation of the DPD exemption, unlimited accessibility may not necessarily mean that an individual's activities fall outside the exemption. For example, version 56 of the proposed GDPR, which was leaked in December 2011, and which formed the basis of consultations with the Directorate Generals, specifically provided that the household exemption would not apply where personal data is 'made accessible to an indefinite number of individuals'.[55]

5.4.2. Data Controller

The proposed GDPR imposes regulatory obligations on 'controllers', with a 'controller' being defined by Article 4(5), in essentially identical terms to the equivalent definition in the DPD, to mean:

> the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data.[56]

---

53 DPD, Article 3(2).

54 *Bodil Lindqvist* (C101/01) [2003] ECR I-12971.

55 European Commission, Proposal for a Regulation of the European Parliament and of the Council *on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* Version 56, 29 November 2011, Article 2(5)(b), Retrieved from http://www.statewwatch.org/news/2011/dec/eu-com-draft-dp-inter-service-consultation.pdf.

56 See DPD, Article 2(d).

A 2010 Article 29 Working Party Opinion on the concepts of 'controller' and 'processor' under the DPD recognised that the definition was difficult to apply in complex environments, such as the use of SNS.[57] In the 2009 Opinion on online social networking, the Working Party concluded that:

- SNS providers that provide online platforms which enable individuals to publish and exchange information with other users are data controllers since they determine the purposes and means of the processing of such data; and
- individual users that upload third party personal data are also data controllers, provided they are not entitled to the 'household exemption'.

These conclusions would appear to apply equally to the definition of 'controller' in the proposed GDPR. It therefore appears that, where an individual is not entitled to the household exemption, the SNS provider and the individual user will be joint controllers. The allocation of responsibilities between joint controllers is expressly addressed in Article 24 of the proposed GDPR, which requires the respective responsibilities of joint controllers to be determined by means of an arrangement between them. This effectively means that, where the household exemption does not apply, the respective responsibilities of SNS providers and individual users for deleting information must be determined by an agreement. Where the household exemption does apply, however, the SNS provider will be solely responsible for deleting information where the Article 17 right to be forgotten is exercised.

6. CONCLUSION

The proliferation of ubiquitous digital traces in networked environments poses fundamental challenges for identity-formation, privacy and autonomy in contemporary societies. These challenges are associated with the persistence of digital information, its ready replicability and its accessibility, especially by search functionality. The use of personal information that is shared in one context by people who form judgments in an entirely different context has the potential to cause significant tangible harms. Moreover, as individual identities become more fragile and fragmented in 'liquid' societies, associated with the erosion of offline communities, the availability of ubiquitous personal information threatens to further undermine individual autonomy and self-determination, including the ability of individuals to sustain long-term relationships. While we are witnessing some corrosion of former borders between private and public, there are no indications of an increase in social tolerance as, paradoxically, the more private information is revealed, the more judgmental some social attitudes appear to become. All of this suggests that there is a pressing need to give individuals greater control of their digital traces, extending to the ability to delete information.

Although some have suggested that greater control can be achieved through market-based or technology-based solutions, neither approach is, at least in isolation, desirable or

57 Article 29 Data Protection Working Party (2010), 2.

workable. Self help, such as through the use of reputation management services, cannot compel the deletion of information and, in any case, is not based on a principled balance between privacy and freedom of expression. Similarly, technology-based solutions are difficult to implement, are susceptible to circumvention, and fail to adequately balance privacy and freedom of expression. Given that the central concerns relating to individual control of persistent digital traces concern identity-formation, privacy and autonomy, the preferred approach is to introduce legal protection through a privacy rights-based framework. Furthermore, just as data protection laws were introduced to establish a balance between privacy and the free flow of personal data in the contexts of ubiquitous data processing by government and private enterprises, so the data protection framework can be adapted to deal with the near-ubiquitous circulation of personal data generated by individuals using Web 2.0 applications, such as SNS. Provided this framework is appropriately adapted, it incorporates established mechanisms for balancing the protection of privacy rights with other rights and interests, especially the right to freedom of expression.

An analysis of the history of data protection law reveals that, while there were early proposals to require the erasure of personal data, fully-fledged deletion rights were not introduced, largely because of concerns that data retention was needed for the benefit of data subjects, and about the potential costs to data controllers. Although it has been suggested that the proposed GDPR strengthens deletion rights already found in the DPD, an examination of the DPD reveals that the existing rights are limited and qualified, and fail to fully implement the deletion principle. On the other hand, the GDPR, which, for the first time proposes to introduce a distinct right to be forgotten, effectively increases the rights of data subjects, by removing or weakening many of the limitations and qualifications found in the DPD, to such an extent that it can be seen as finally recognising the deletion principle.

Although the GDPR implements the deletion principle, the right to be forgotten is subject to important exceptions and limitations, which are intended to protect countervailing interests and rights, and especially the right to freedom of expression. If, as this paper has argued, there is a strong case for equipping individuals with greater rights to control their personal data, the appropriate balance between privacy and freedom of expression is best set through a rights-based framework. While the GDPR, against the backdrop of European human rights law, establishes a firm foundation for appropriately balancing rights and interests, there remain significant ambiguities and uncertainties with the proposed instrument, some of which could be reduced by relatively minor amendments.

First, as the EDPS pointed out, uncertainty arising from the ability of Member States to override the right to be forgotten pursuant to Article 17(3)(d) could be removed by deleting the exception, as there is no apparent need for national derogations over and above those provided under Article 21. Secondly, as private individuals are now the source of much personal data that is recorded and accessible online, and given the associated blurring of boundaries between private and personal uses and public uses, there are considerable uncertainties about the application of the household exemption to Web 2.0 applications, as well as the extent to which individuals should be regulated as data controllers. Some uncertainty about

the application of the household exemption could be reduced by reverting to the earlier draft proposal, which would ensure that it is not available where an individual makes personal data 'accessible to an indefinite number of individuals'. Such an amendment may also assist in determining the key issue of when individuals should be regulated as data controllers.

To an extent, there is some scope for mechanisms established under the GDPR - such as the possibility of the proposed European Data Protection Board (EDPB) issuing guidelines, recommendations or best practices[58] - to be used to clarify what seem likely to be complex, ongoing issues. In this respect, it should be noted that, while the EDPS and Working Party have both expressed reservations about the proposed powers of the Commission to adopt delegated and implementing acts,[59] similar concerns are not expressed about the powers of the proposed EDPB. Finally, quite apart from the proposed recognition of a right to be forgotten under the GDPR, it is seems that the legal parameters of the right will be clarified by the extent to which it is interpreted as part of the fundamental right to data protection,[60] in proceedings such as the referral of complaints against Google to the Court of Justice of the EU (ECJ) by a Spanish Court, mentioned above.[61] It may well be that the potentially complex path to the implementation of the proposed new data protection framework, including the right to be forgotten, will be significantly influenced by forthcoming decisions from the ECJ.

7. BIBLIOGRAPHY

Article 29 Data Protection Working Party. (2009a). *The Future of Privacy,* Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, Adopted on 1 December 2009, 02356/09/EN, WP 168.

Article 29 Data Protection Working Party. (2009b). *Opinion 5/2009 on online social networking,* Adopted on 12 June 2009, 01189/09/EN, WP 163.

Article 29 Data Protection Working Party. (2010). *Opinion 1/2010 on the concepts of «controller» and «processor»,* Adopted on 16 February 2010, 00264/10/EN, WP 169.

Article 29 Data Protection Working Party. (2012). *Opinion 1/2012 on the data protection reform proposals,* Adopted on 23 March 2012, 00530/12/EN, WP 191.

Bartow, A. (2009). Internet Defamation as Profit Center: The Monetization of Online Harassment. *Harvard Journal of Law & Gender,* 32, 383-429.

Bauman, Z. (2000). *Liquid Modernity.* Cambridge, UK: Polity Press.

58 Proposed GDPR, Article 66(1)(b).

59 Article 29 Data Protection Working Party (2012); European Data Protection Supervisor (2012).

60 See Charter of Fundamental Rights of the EU, Article 8; Treaty of the Functioning of the European Union, Article 16(1).

61 See note 7.

Bauman, Z. (2004). *Identity.* Cambridge, UK: Polity Press.

Bauman, Z. (2007). From Pilgrim to Tourist – or a Short History of Identity. In Jiří Přibáň (ed.), *Liquid Society and its Law* (pp. 18-36). Aldershot, UK: Ashgate.

Bauman, Z. (2011). Privacy, Secrecy, Intimacy, Human Bonds – and Other Collateral Casualties of Liquid Modernity. *The Hedgehog Review.* Spring 2011, 20-29.

Boyd, D. (2010). Social Networked Sites as Networked Publics: Affordances, Dynamics, and Implications. In Zizi Papacharissi (ed.), *Networked Self: Identity, Community, and Culture on Social Network Sites* (pp. 39-58). New York: Routledge.

Bygrave, L. (2002). *Data Protection Law: Approaching Its Rationale, Logic and Limits.* The Hague: Kluwer Law International.

Cate, F.H. (2006). The Failure of Fair Information Practices Principles. In Jane K. Winn (ed.), *Consumer Protection in the Age of the «Information Economy»* (pp. 341-378) Surrey, UK: Ashgate.

de Terwangne, C. (2012). Internet Privacy and the Right to be Forgotten/Right to Oblivion. [online monograph] *IDP. Revista de Internet, Derecho y Política.* No. 13, pp. 109-121. UOC. Retrieved April 25th 2012 from http://idp.uoc.edu/ojs/index.php/idp/article/view/n13_terwangne_esp/n13_terwangne_eng.

Dumortier, K. (2009). Facebook and Risks of «De-contextualization» of Information. [online monograph] *IDP. Revista de Internet, Derecho y Política.* No. 9, pp. 1-16. UOC. Retrieved April 25th 2012 from http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_dumortier/n9_dumortier_eng.

European Commission. (2010). *A comprehensive approach on personal data protection in the European Union,* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final. Brussels, 4 November 2010.

European Commission. (2011). Proposal for a Regulation of the European Parliament and of the Council *on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* Version 56, 29 November 2011. Retrieved April 25th 2012 from http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-inter-service-consultation.pdf.

European Commission. (2012). *Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century,* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 9 final. Brussels, 25 January 2012.

European Data Protection Supervisor. (2012). *Opinion of the European Data Protection Supervisor on the data protection reform package,* 7 March 2012.

Goffman, E. (1961). *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates.* New York: Anchor Books.

Johnson, B. (2010). *Privacy no longer a social norm, says Facebook founder,* 11 January 2010. Retrieved March 20th 2012 from http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy.

Keele, B.J. (2009). Privacy by Deletion: The Need for a Global Data Deletion Principle. *Indiana Journal of Global Legal Studies,* 16(1), 363-384.

Kirby, M. (1980). Transborder Data Flows and the «Basic Rules» of Data Privacy. *Stanford Journal of International Law.* 16, 27-66.

Kirby, M. (1991). Legal Aspects of Transborder Data Flows. *Computer/Law Journal,* 11, 233-245.

Koops, B-J. (2011). Forgetting Footprints, Shunning Shadows. A Critical Analysis of the «Right to be Forgotten» in Big Data Practice. *script*ed, 8(3), 229-256.

Levy, S. (2011). *In the Plex.* New York: Simon & Schuster.

Lindsay, D. (2005). An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law. *Melbourne University Law Review,* 29, 132-178.

Mayer-Schönberger, V. (2009). *delete: The Virtue of Forgetting in the Digital Age.* Princeton, NJ: Princeton University Press.

Nagel, T. (1998). Concealment and Exposure. *Philosophy and Public Affairs,* 27(1), 3-30.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review,* 79(1), 119-157.

Peguera, M. (2012). *Spain asks the ECJ whether Google must delete links to personal data, March 2, 2012.* Retrieved March 24th, 2012 from http://ispliability.wordpress.com/

Přibáň, J. (2007). Introduction: Theorizing Liquid Modernity and its Legal Context. In Jiří Přibáň (ed.), *Liquid Society and its Law* (pp. 1-14). Aldershot, UK: Ashgate.

Rachels, J. (1975). Why Privacy is Important. *Philosophy and Public Affairs,* 4, 323-33.

Reding, V. (2011). The upcoming data protection reform for the European Union. *International Data Privacy Law,* 1(1), 3-5.

Reiman, J.H. (1976). Privacy, Intimacy, and Personhood. *Philosophy and Public Affairs,* 6, 26-44.

Rosen, J. (2010). The End of Forgetting. *The New York Times Magazine,* July 25, 2010, 32-45.

Secretary's Advisory Committee on Automated Personal Data Systems, United States Department of Health, Education and Welfare (1973). *Records, Computers and the Rights of Citizens.* Retrieved March 19th 2012 from http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

Simitis, S. (1987). Reviewing Privacy in an Information Society. *University of Pennsylvania Law Review,* 135, 707-746.

Solove, D.J. (2007). *The Future of Reputation.* New Haven and London: Yale University Press.

Vaidhyanathan, S. (2011). *The Googlization of Everything (And Why We Should Worry).* Berkeley, Cal.: University of California Press.

Warner, J. (2005). The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps. *University of Ottawa Law & Technology Journal,* 2, 75-104.

Weber, R.H. (2011). The Right to Be Forgotten: More Than a Pandora's Box. *Journal of Intellectual Property, Information Technology and E-Commerce Law,* 2(2), 120-130.

Werro, F. (2009). The Right to Inform v. The Right to be Forgotten: A Transatlatic Crash. In Aurelio Colombi Ciacchi, Christine Godt, Peter Rott and Leslie Jane Smith (eds.), *Liability in the Third Millenium* (pp. 285-300). Baden-Baden, FRG: Nomos.

NUEVOS RETOS DE LA REGULACIÓN JURÍDICA Y DEONTOLÓGICA DE LA PUBLICIDAD EN LAS REDES SOCIALES

Esther Martínez Pastor
Prof. Contratado Doctor. Universidad Rey Juan Carlos
Mercedes Muñoz Saldaña
Prof. Contratado Doctor. Universidad de Navarra

RESUMEN: Esta investigación pretende exponer algunos asuntos sobre la problemática que plantean las nuevas prácticas publicitarias en la red en relación con los derechos de sus usuarios. La publicidad en Internet, al contrario que su regulación, se ha desarrollado de forma vertiginosa. Las empresas apuestan por una publicidad personalizada para dirigir mejor las ofertas publicitarias a sus potenciales clientes; sin embargo, la protección jurídica de los derechos de los usuarios en este proceso parece escasa o poco efectiva. Este problema se ha incrementado con el desarrollo de las redes sociales ya que la gestión de los datos permite a los anunciantes identificar a sus clientes con una segmentación ad hoc, de acuerdo con los perfiles que ellos mismos editan y en los que incluyen datos tanto personales como relativos a sus amigos o entorno cercano. La recopilación de estos datos permite, gracias a la información sobre la navegación, elaborar informes estadísticos de consumo en la red y segmentar y personalizar la publicidad insertada; sin embargo, cuanto más exitoso es este proceso, más comprometida puede verse la intimidad del usuario. Nos encontramos en un período de búsqueda de soluciones en el necesario y urgente equilibrio entre el desarrollo de la publicidad y la protección de los usuarios en las redes sociales.

PALABRAS CLAVE: autorregulación, regulación, publicidad, redes sociales, datos personales.

1. PUBLICIDAD EN LA RED, INTIMIDAD Y DATOS PERSONALES. EL RETO DEL EQUILIBRIO

La realidad es tozuda y por eso podemos afirmar que la publicidad ha llegado a Internet para quedarse y crecer. En un contexto de crisis mundial materializada en un descenso de la inversión publicitaria en todos los soportes, la publicidad en la red sigue creciendo. La causa: en abril de 2011 Europa contaba con 365,3 millones de usuarios en Internet. A nivel mundial la cifra asciende a 1.362 millones de usuarios únicos con una media de conexión de 24,2 horas por persona. En el uso de redes sociales, Facebook, en noviembre de 2011, contaba con 800 millones de usuarios en el mundo y Twitter, en septiembre del mismo año, sumaba 200 millones de usuarios registrados. En cuanto a la inversión publicitaria en redes sociales se prevee prevé que para 2013 supere los 10.000 millones de dólares y represente el 9,4 por ciento de la tarta para publicidad en Internet. Las redes sociales preferidas para invertir son Facebook, Twitter o y Likedin. Facebook está a la cabeza con una inversión del 72% frente a las demás redes sociales y los expertos prevén que en 2012 esta red obtendrá el 6,1% del gasto mundial de publicidad en la red.

La publicidad tiene como objetivo llegar a la audiencia de la manera más directa y personalizada posible y la red resulta un medio especialmente idóneo para ello. En el caso de las redes sociales, con el acceso a la información volcada en ellas, se consigue no sólo una contextualización de los contenidos publicitarios, la cual ya estaba presente aunque en menor medida en los soportes tradicionales; sino una radical personalización de la publicidad insertada, de tal forma que, como se ha señalado, no se trata sólo de que los anuncios guarden una relación con las palabras introducidas en un buscador concreto o con el contenido de la página que se visita; sino que la publicidad «se sirve de información que el sitio *web* o el proveedor de anuncios tiene sobre las circunstancias particulares del usuario en cuestión». Es la denominada *online behavioural advertising* mediante la cual, cuanta más información se disponga de dicho usuario, más personalizado será el mensaje insertado y, al mismo tiempo, más comprometida se verá la privacidad del mismo.

Existen distintas maneras de ofrecer publicidad basada en el comportamiento. En un nivel básico la información relativa a la navegación de cada usuario se recopila, guarda y categoriza en diferentes grupos de productos o servicios como, por ejemplo, coches o viajes, los cuales se asocian con los datos sobre los sitios web que se han visitado. Esto es posible gracias a las *cookies* que se instalan en un fichero en los dispositivos que tienen acceso a la red. De esta manera los anunciantes afinan la detección de las necesidades de su público objetivo ofreciéndole anuncios dirigidos a sus gustos y preferencias. Por ello, el acceso, tratamiento y difusión de datos personales resulta la clave en este proceso.

Hay que partir de la existencia de niveles o grados en el acceso y utilización de datos personales de los usuarios con fines publicitarios de tal forma que la información a la que se accede mediante las *cookies* de los sitios *web* se puede considerar necesaria para su funcionamiento y, por tanto, no tiene por qué ser problemática desde el punto de vista del tratamiento de los datos con fines publicitarios; mientras que las *cookies* empleadas por las redes de publicidad u otros sistemas propios de gestión publicitaria de las redes sociales, son capaces de rastrear el comportamiento de los internautas de tal forma que su navegación deja un historial con el cual dichas redes construyen un perfil del usuario, por otra parte ajeno este proceso, cuya concreción depende de la actividad realizada en los sitios web que visita. Siguiendo dicha gradación, el problema se agudiza cuando la información sobre el usuario se consigue directamente de proveedores de servicios de Internet o ISP's ya que estos contienen toda la información sobre nuestra actividad completa en la red.

2. LOS TRES EJES PARA EL EQUILIBRIO: LA PRESTACIÓN DEL CONSENTIMIENTO; EL DERECHO A LA INFORMACIÓN Y EL DERECHO DE OPOSICIÓN

A pesar de que las empresas proveedoras de publicidad en Internet insisten en que los datos recopilados no permiten identificar personalmente al usuario, sino únicamente detectar sus gustos e intereses de acuerdo con unos parámetros de navegación y/o búsqueda en Internet, resulta imposible obviar que dicha navegación y los datos personales difundidos en ella posibilitan dicha identificación con relativa facilidad y deja en manos de las políticas

empresariales y de la ética profesional el utilizarlos con fines publicitarios. En cualquier caso, lo que sí resulta clave en las prácticas publicitarias en Internet es el desconocimiento por parte del usuario del almacenamiento y uso de los datos personales con fines publicitarios fruto su actividad en la red. En una visión global y resumida, los principios que sustentan el marco jurídico del tratamiento de datos personales con fines publicitarios en la red son tres: la prestación del consentimiento, el derecho de información y el derecho de oposición.

2.1. Prestación del consentimiento

En cuanto al consentimiento, uno de los principales problemas que plantea este escenario es que son los usuarios los que ponen a disposición de un grupo cerrado o abierto (en ocasiones ilimitado) de receptores datos referentes a su vida privada; mientras que, como se ha señalado, la legislación va destinada a regular el tratamiento de dicha información por parte de empresas y de proveedores. Ante esta realidad, sin renunciar a las medidas legales oportunas que se puedan aplicar, la solución implica a los propios usuarios mediante un «uso diligente» de las redes sociales lo cual precisa una adecuada alfabetización digital de los usuarios respecto de dicho uso. En especial, en el caso de menores y jóvenes ya que existe una cierta «perdida de conciencia sobre el valor de la vida privada personal».

Por otra parte, como expone el Eurobarómetro de junio de 2011 sobre la protección de datos y la identidad electrónica en las redes sociales existe una cierta obligación de divulgar determinada información personal si el usuario quiere acceder a determinados servicios a través de Internet, como el correo electrónico o el acceso a determinada información. Por tanto, resulta cierto que a través de c*ookies* que permiten personalizar el servicio y también la publicidad, el usuario paga con los datos relativos a su intimidad el acceso a determinadas aplicaciones, en su mayoría, aparentemente gratuitas.

En cualquier caso, la legislación dispone que, como norma general, el tratamiento de datos personales, también o incluso especialmente con fines publicitarios, precisa el consentimiento de la persona afectada, entendiendo como tal «toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. Así, únicamente se permite «el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE».

2.2. Derecho de Información

Directamente relacionado con el consentimiento, se sitúa el principio del Derecho de información de los titulares de datos personales sometidos a tratamiento con fines publicitarios. Cabe preguntarse, ¿le preocupa o molesta al usuario dicha utilización? ¿Es consciente de dicho uso así como de los derechos que le asisten cuando se registra, por ejemplo, en una red social? Algunas de las respuestas vertidas en los últimos estudios resultan indicativas al

respecto. El 70% de los encuestados al respecto entre noviembre y diciembre de 2010 se mostraba disconforme con dicho uso. Por otra parte, aunque en lo referente a la relación entre publicidad y redes sociales y a la percepción de los usuarios de las mismas, según Digital Life 2011 «el 53% de los usuarios de redes sociales a nivel mundial no quiere relacionarse con marcas a través de ellas, porcentaje similar en nuestro país. La cifra alcanza el 60% en EEUU y el 61% en UK».

Por tanto, podemos decir que contrasta la percepción de los usuarios sobre su relación con la publicidad, por ejemplo, a través de las redes sociales bien sea de manera directa o indirecta y el masivo uso de los datos personales vertidos en ellas con fines publicitarios o las inversiones millonarias de las marcas en este ámbito.

La cuestión es que la satisfacción del derecho de información sobre el uso de los datos personales que volcamos en la red incluye el derecho a ser informado de manera expresa, precisa e inequívoca sobre: la identidad del responsable del tratamiento; los fines del tratamiento de que van a ser objeto los datos; los destinatarios o las categorías de destinatarios de los datos; el derecho de oposición o la existencia de derechos de acceso y rectificación de los datos que le conciernen.

La Directiva sobre privacidad y comunicaciones electrónicas también incide en esta cuestión al resaltar que el consentimiento está supeditado a que se le haya proporcionado al usuario «una información clara y completa sobre los fines del tratamiento de los datos». Por esta cuestión, al referirse en sus considerandos a la instalación de *cookies* especifica que, aún pudiendo constituir un instrumento legítimo y de gran utilidad, debe proporcionarse a los usuarios información «clara y precisa» para garantizar que los mismos son conscientes de la información que se introduce en el equipo terminal que están utilizando. Así, se debe garantizar la posibilidad de impedir «que se almacene en su equipo terminal un «chivato» (cookie) o dispositivo semejante».

De acuerdo estos principios, el Dictamen 5/2009 sobre redes sociales *on line* advierte que, los proveedores de estos servicios tienen la obligación de adoptar, en el momento del registro de un usuario a la red social las medidas oportunas para mantener la seguridad de los datos aportados e impedir accesos no autorizados «implantando por defecto medidas de seguridad protectoras ya que la gran mayoría de los usuarios no realizarán cambios en un futuro en esa configuración». Sin embargo, como habitualmente se suele señalar, las medidas asumidas por defecto suelen ser las menos protectoras para la privacidad del usuario.

Además, el principio de información se suele satisfacer de manera confusa, en muchos casos ininteligible para el consumidor, y ambigua, de tal forma que el consentimiento no se puede considerar como un consentimiento informado. Por otra parte, los cambios repentinos en las políticas de privacidad exigen una renovación del consentimiento y, por lo tanto, una nueva satisfacción del derecho de información de acuerdo con las nuevas condiciones de privacidad.

Por ello, y en aras de avanzar en el cumplimiento de este derecho de información, las últimas aportaciones abogan por el criterio de la transparencia en la presentación de dicha información ya que su inclusión en la política de privacidad, en letra pequeña y al final de la página, no suele ser en la mayoría de las ocasiones una manera eficaz de informar

al usuario sobre los derechos que le asisten y, además, en la mayoría de las ocasiones, su redacción resulta ininteligible para un usuario medio que, en gran medida, desconoce el marco legal.

Por este motivo la Comisaria Viviane Reding ha insistido en que la *Privacy by Design* es el punto de encuentro entre los intereses de la industria y de los ciudadanos/usuarios de las Redes Sociales. La política de *Privacy by Desing* supone tener presente el derecho a la privacidad del usuario como un elemento capital desde la configuración y el diseño de la red social hasta el fin de su uso por parte del usuario.

Como se ha señalado, teniendo en cuenta que la ley es cada vez más concreta e insistente respecto de este punto, quizá convenga desterrar la idea de que es mejor esconder dichas prácticas por temor a que el usuario se oponga al tratamiento de sus datos con fines publicitarios con lo que ello conllevaría. La realidad puede ser sorprendente y demostrar que una información clara y sencilla sobre el funcionamiento de la publicidad personalizada a través de internet y de sus ventajas para el usuario puede ser eficaz en una estrategia a medio-largo plazo basada en una relación de interés mutuo y confianza entre las empresas-marcas y sus potenciales consumidores.

2.3. Derecho de oposición

En cualquier tratamiento de datos con fines publicitarios permanece el derecho de oposición de usuario, el cual implica el derecho a negarse, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa.

La versión actualizada de la Directiva sobre privacidad y comunicaciones electrónicas cuestiona la práctica habitual de asumir como válido el que la ausencia de negativa para por parte del usuario implica una aceptación de dichas prácticas. La ley exige un consentimiento que, como recogía la normativa sobre protección de datos, sea informado e inequívoco

La dificultad se plantea por varios frentes: el escaso conocimiento que a día de hoy tiene el usuario sobre las posibilidades en la configuración del nivel de privacidad de su navegador; la dificultad que dichas acciones puede generar en la propia navegación; o la de acceder a un sistema que permita ejercer este derecho de manera efectiva y permanente.

En cualquier caso, la legislación apunta que garantizar el derecho de oposición del usuario es un requisito esencial para la legalidad de dichas prácticas, por lo que dichas dificultades deben ser superadas si se quiere hacer cumplir la normativa jurídica recientemente aprobada.

Por ello parece conveniente invertir en una pedagogía sencilla y completa al mismo tiempo sobre el funcionamiento de la publicidad en Internet, y más en concreto en las redes sociales, y de los derechos y deberes de los usuarios respecto de la protección de su intimidad y sus datos personales en el tratamiento de datos con fines publicitarios. Por otra parte, si el usuario es consciente de los riesgos que corre al difundir determinada información a través de la red probablemente se vuelva más cauteloso y consigamos recuperar, al menos en parte, esa conciencia de privacidad que parece haberse perdido.

3. LA REGULACIÓN COMO PUNTO DE PARTIDA Y LA CORREGULACIÓN COMO DESARROLLO DE LA AUTORREGULACIÓN

En el ámbito europeo la legislación que afecta al tema de la privacidad y los datos personales en la práctica publicitaria a través de la red se encuentran en la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (en adelante, Directiva sobre la privacidad y las comunicaciones electrónicas) y en la Directiva 1995/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos (en adelante, Directiva sobre Protección de Datos).

Estos textos se fundamentan en los principios recogidos en la Carta Europea de Derechos Fundamentales, en concreto, en su artículo 7 «Respeto de la vida privada y familiar» en el que se dispone que «toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones» y en su artículo 8 «Protección de datos de carácter personal» que reconoce el derecho de toda persona a: la «protección de los datos de carácter personal que la conciernan; a un tratamiento de los mismos de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley»; al derecho a acceder a los datos recogidos que la conciernan y a su rectificación; y al respecto de dichas normas bajo el control de una autoridad independiente.

En relación directa con la Directiva sobre Protección de Datos, sometida en estos meses a un proceso de actualización, cabe destacar la intensa y fructífera labor realizada por el Grupo de Trabajo del artículo 29 (GT 29). Dicho Grupo se creó en 2003 en virtud de lo dispuesto en el artículo 29 de dicha Directiva. Se trata de un organismo de la UE, con carácter consultivo e independiente, cuya labor se centra en salvaguarda de la protección de datos y del derecho a la intimidad en el ejercicio de las comunicaciones electrónicas. Sus funciones se describen en el artículo 30 de la Directiva sobre Protección de Datos y en el artículo 14 de la Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

Por ejemplo, en lo referente a la publicidad comportamental en línea, una de las más notables y recientes contribuciones del GT 29 ha sido el Dictamen 2/2010 de 22 junio de 2010. En este Dictamen se insta a que los proveedores de redes de publicidad creen mecanismos de autorización previos a la instalación de *cookies* o similares y a su posterior seguimiento, de acuerdo con lo dispuesto en la Directiva sobre privacidad de las comunicaciones electrónicas y con la Directiva sobre Protección de Datos. En primer lugar, de acuerdo con lo dispuesto en la Directiva sobre privacidad, los usuarios tienen derecho a conocer la información que será almacenada en sus dispositivos de acceso a Internet y, que posteriormente, será utilizada para obtener información sobre su navegación. Así, la Directiva protege la intimidad de cada usuario entendiendo que los terminales son una extensión de su esfera

privada, dejando de lado si los datos almacenados en ellos son personales o no. De otro lado, la Directiva sobre Protección de Datos salvaguarda la información recabada a través de la navegación de los usuarios en su condición de datos personales.

Otro punto importante del Dictamen 2/2010 consiste en la identificación y asunción de responsabilidades de los tres sujetos que participan en la publicidad comportamental, a saber, los proveedores de redes de publicidad, los anunciantes y los editores. Los proveedores de redes de publicidad, que son los distribuidores de la misma, deben obtener el consentimiento de los usuarios para almacenar y gestionar la información de la navegación a través de las *cookies* o similares. Por su parte, los anunciantes deben solicitar el consentimiento de los usuarios para ofrecer una publicidad personalizada previa adquisición de datos gracias al rastreo de su navegación. Y los editores, los cuales difunden la publicidad mediante las webs, pueden ser responsables del tratamiento de datos de carácter personal por configurar sus sitios de tal forma que los buscadores de los visitantes sean redireccionados automáticamente a la página web del preveedor proveedor de redes de publicidad (que les envía una *cookie* y publicidad a medida).

El GT 29 insiste en la necesidad de informar al usuario, de que éste ofrezca su consentimiento previo a este tipo de publicidad y propone que «en el caso de las *cookies*, debería informarse cuando está previsto que el software de internet reciba, almacene o envíe una *cookie*. El mensaje deberá especificar, en un lenguaje comprensible, qué información se pretende almacenar en la *cookie* y con qué objeto así como el período de validez de la *cookie*».

La respuesta a las demandas previstas en el ámbito normativo se ha concretado en la iniciativa de la EASAE/IAB, la cual lanzó en abril de 2011 un Código de Autorregulación Sobre las Buenas Prácticas de la Online Behavioural Advertising. Este Código pretende afrontar lo dispuesto en el Dictamen 2/2010 en el que se animaba al sector industrial a participar en la corregulación de este tipo de publicidad. En esta propuesta el sector privado: anima a los usuarios a elegir si quieren recibir publicidad motivacional; propone la aparición de un icono cada vez que aparezca la publicidad comportamental en el que se pueda cliquear; y que éste vincule a una web en la que se explica esta modalidad publicitaria (www.youronlinechoices.eu). Sin embargo el GT 29 ha emitido un nuevo Dictamen 26/2011 sobre el Código de Buenas Prácticas en materia de publicidad comportamental en línea EASA/IAB en el que concluye que este Código de Autorregulación no parece ajustarse del todo al contenido de la Directiva sobre privacidad y comunicaciones electrónicas ni a lo dispuesto en el Dictamen 2/2010 sobre Publicidad comportamental. Según el GT 29 al usuario no se le ofrece la posibilidad de dar su consentimiento antes de recibir dicha publicidad, sino únicamente después. Primero se le sigue y después se le informa, contrariamente a lo que disponen la normativa europea. Además, el icono no informa sobre el rastreo de la navegación y almacenamiento de datos con la finalidad de compartirlos con otras empresas y, posteriormente, ofrecer anuncios personalizados. Por último, el GT 29 considera que ni el icono ni el sitio web habilitado proporcionan una fácil comprensión sobre esta publicidad y tampoco sobre sus efectos.

La realidad es que este Código de Buenas Prácticas, aún siendo un paso adelante, se sitúa en el ámbito de la autorregulación más que en las nuevas iniciativas de corregulación

solicitadas desde las instancias europeas. La corregulación, como desarrollo de la autorregulación, es un instrumento capaz de desarrollar los presupuestos del marco legal, contando de manera activa con la colaboración de los representantes de las diferentes partes implicadas, bajo la supervisión de las Autoridades correspondientes y asumiendo consecuencias concretas en caso de incumplimiento. La corregulación implicaría la participación de las autoridades en las medidas adoptadas y una serie de acuerdos previos a la publicación de dicho Código, tanto sobre el contenido como sobre el procedimiento de su aplicación y de las posibles causas de su incumplimiento.

Así desde la corregulación, por un lado, se puede dotar de eficacia al cumplimiento del marco legal y, además, se puede avanzar, en los caminos propuestos como: *privacy by desing-design*; obligaciones de transparencia; o educación del usuario sobre derechos y deberes en el uso de las redes sociales. Sin embargo, la corregulación exige el acuerdo entre el sector público y el industrial. A día de hoy, las instituciones europeas buscan proteger los derechos de los usuarios, mientras que el sector privado se empeña en interpretar de manera laxa la protección de los navegantes, de acuerdo con sus propuestas de autorregulación. Lo que parece claro es que un enfrentamiento entre ambos sólo conduce a que estas prácticas continúen y a que las soluciones se retrasen, priorizando intereses que, habitualmente, no pertenecen a los usuarios. Aunque, recientemente existe una carta del GT29 a EASA invitando a la industria a reunirse en el W3C que puede ayudar a mejorar el panorama publicitario on line.

4. BIBLIOGRAFÍA

EASA-IAB (2012). Guía sobre publicidad basada en el comportamiento. Recuperado el 16 de marzo de 2012 en: http://www.youronlinechoices.com/es/preguntas-frecuentes

EASA/IAB (2012), *Código de Autorregulación Sobre las Buenas Prácticas de la Online Behavioural Advertising*. Recueprado el 1 de marzo de 2012 en: www.iabeurope.eu

Datos comScore Releases European Engagement and Top Web Properties Rankings for April 2011 (2011). Recuperado el 1 de marzo de 2012 en: http://www.comscore.com/Press_Events/Press_Releases/2011/6/comScore_Releases_European_Engagement_and_Top_Web_Properties_Rankings_for_April_2011

FTC Staff Report (2009). *Self Regulatory Principles for online behavioral advertising*. Recuperado el 27 de febrero de 2012 en: http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf

Special Eurobarometer (2011). *Attitudes on Data Protection and Electronic Indetity un the European Union*. Recuperado el 1 de marzo de 2012 en http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

TNS (2011). *Digital life 2011.Informe global*. Recuperado el 15 de febrero de 2012 en: http://www.comunicar.info/2011/11/digital-life-2011-informe-global-de-tns.html

Azurmendi, A. (2011). *Derecho de la Comunicación*. Barcelona: Bosch

Graham R. and Shelton D. (2011). «Online behavioural advertising: the gathering US and European Union storm». *Intermedia*, vol. 39, pp. 27- 41.

Gutíerrez R. (2011). *La inversión publicitaria en Internet aumenta un 8'5%*. Recuperado el 21 de marzo de 2012 en: http://www.eleconomista.es/interstitial/volver/animales/empresas-finanzas/noticias/3478114/10/11/La-inversion-publicitaria-en-Internet-aumenta-un-85-.html

Muñoz Saldaña, M. (2011). «Código CoAN 2010: el primer Código de Corregulación Audiovisual de España». *Revista Latina de Comunicación Social*, vol (66), pp. 235-251.

Ortega Jiménez, A. (2010). Derecho Internacional Privado, Protección de Datos y Redes Sociales en Internet. En Rallo Lombarte, A. y Martínez Martínez, R. (Coord.). *Derecho y Redes Sociales.* Cizur Menor (Navarra): Aranzadi.

Ortíz López, P. (2010). «Redes Sociales: funcionamiento y tratamiento de información personal». En Rallo Lombarte, A. y Martínez Martínez, R. (Coord.). *Derecho y Redes Sociales.* Cizur Menor (Navarra): Aranzadi.

Peguera Poch, M. (2010). «Publicidad online basada en comportamiento y protección de la privacidad». En Rallo Lombarte, A. y Martínez Martínez, R. (Coord.). *Derecho y Redes Sociales.* Cizur Menor (Navarra): Aranzadi.

Reding, V. (2010), *Privacy: the challenges ahead for the European Union*. Recuperado el 8 de marzo de 2012 en: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/16&format=HTML&aged=0&language=EN&guiLanguage=en

Directiva 2002/58/CE, de 12 de Julio de 2002, relativa al tratamiento de los datos personales y La protección de la intimidad en el sector de las comunicaciones electrónicas, DO L 201 de 31.7.2002, p. 37. Versión actualizada y modificada por la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 (DO L 105, de 13.4.2006, p. 54 y ss) y por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 (DO L 337, de 18.12.2009, p. 11 y ss).

Directiva 1995/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, (DO L 281 de 23.11.1995, p. 31). Modificada por el Reglamento (CE) nº 1882/2003 del Parlamento Europeo y del Consejo de 29 de septiembre de 2003, DO L 284, de 31.10.2003, p.1

Grupo de trabajo sobre protección de datos (2000). *Privacidad en Internet-Enfoque Integrado de Protección de Datos Online*, (WP 37). Recuperado el 2 de marzo de 2012 en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37es.pdf

Grupo de trabajo sobre protección de datos (2002). *Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE,* (WP 56). Recuperado el 2 de marzo de 2012 en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_es.pdf

Grupo de Trabajo sobre Protección de Datos (1999). *Recomendación 1/99 sobre el tratamiento invisible y automático de los datos personales en Internet* .(WP 17). Recuperado el 18

de marzo de 2012 en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp17es.pdf

Grupo de Trabajo sobre protección de datos (2009). *Opinion 5/2009 on online social networking* (WP 163). Recuperado el 6 de febrero de 2012 en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/2009/common/wp163_en.pdf

Grupo de Trabajo sobre Protección de Datos (2010). *Dictamen 2/2010 sobre Publicidad comportamental en línea*. Recuperado el 9 de marzo de 2012 en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_es.pdf

Grupo de Trabajo sobre Protección de Datos (2011). *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*. Recuperado el 20 de marzo de 2012 en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf

NAMING AND SHAMING IN GREECE: SOCIAL CONTROL, LAW ENFORCEMENT AND THE COLLATERAL DAMAGES OF PRIVACY AND DIGNITY

Lilian Mitrou
Associate Professor
Department Information and Communication Systems Engineering
University of the Aegean - Greece

ABSTRACT: This paper addresses the issue of identifying in public the persons that are either arrestees or suspects of crime or tax evaders. Naming and shaming measures have been recently introduced in Greece as a tool for enabling social control and thus achieving purposes of law enforcement. Shaming becomes a formal tactic of punishment itself, signalizing social disgrace and reflecting a shift to the conception of compliance and the role of the society. Shaming interferes with the fundamental rights and liberties of the persons affected. The approach of this paper is that evaders, arrestees and suspects should not be deprived of their rights, especially their rights to informational privacy and dignity. Furthermore shaming publicity may threaten the right to the presumption of innocence. The stigmatizing effect of shaming is enhanced through the technical apparatus, which renders information more easily detected, reproduced, permanently stored, and undermines the right to oblivion and rehabilitation. The invocation of the social control, often as a substitute of proper public action, does not fit into any cognizable notion of state responsibility, while it is not sure that this art of sanction deters future crime and connects the offender and the society to an understanding of lawfulness by internalizing these lawful values. The assumption of this paper is that a democratic, liberal State should treat a person as someone possessing the basic dignity and never humiliate a person by using her as means.

KEYWORDS: naming, shaming, sex offenders, tax evaders, reputation informational privacy, presumption of innocence, dignity.

1. NAMING AND SHAMING: AN INTRODUCTION

Recently, there has been in Greece a considerable public debate about the so-called «naming and shaming» policy, which is implemented mainly in relation to sex/child pornography offenders and tax evaders. In the first case the Greek law provides for the competence of prosecutors to decide on the naming of persons accused or suspected, whereas in the latter case the naming of tax evaders is laid down as an obligation of tax authorities.

Naming the offender constitutes an integral component of shaming policies. In the context of this paper we understand by «naming» the disclosure, publication and dissemination of the identity of a person, who is convicted or suspected of crime or tax evasion. The affected person may be either directly identified or identifiable by reference to factors specific to her identity. Naming magnifies the negative effects inherent in accusation or conviction

through communicating the offender's status and relation to an illegal conduct to a wide public. Publicity serves as means (in order) to shame, reprimand, reproach, censure, control, influence, supervise the person identified as offender [Pawson 2001]. This stigmatizing publicity aims and/or results to raise sentiments of guilt and shame[1].

If shame is considered a private emotional reaction of the wrongdoer, shaming is a social process of purposefully expressing disapproval and/or contempt with the intention or effect of provoking embarrassment, discomfort, anger and –last but not least- fear. Apparently shame and shaming are closely intertwined. Shaming practices expose the offender inflicting personal and psychological as well as social costs on her. Some authors distinguish between stigmatic and reintegrative shaming. Stigmatizing shaming brands the offender and shuns her from society while reintegrative shaming not only involves the community but it also aims at the reintegration of the shamed person back into it [Nussbaum 2004].

Shaming is not a new tool. Shaming, carried on in various ways by state authorities and communities, has been a dubious and pervasive part of punishment throughout history. Romans branded a letter signifying the crime onto the offender's forehead[2]. In ancient Rome, also the doors to the homes of criminals were branded in order to alert the public of the acts of their residents. Harmenopoulos in *Hexabiblos* (Εξάβιβλος), a compilation of byzantine legislation in force in 14th century[3], is referring to the punishment provided for dishonest merchants and contractors, who «after being paraded around, spat and with their heads shaved, have to be sent into exile». Communities have used shaming as a mechanism for preserving civility and social order[4]. Brands and signs were (and still are) intended to announce the spoil identity of the wrongdoer to the world.

Over time, the use of punishments such as the «Scarlet Letter»[5] disappeared as a rejected practice of a foregone era. The Enlightment, the recognition of the dignity of a person as a constitutional value, the rise of the strong central State, which reinforced norms through punishment, and the changes in the structure and nature of communities (urbanization, mobility etc.) formed a new context for judging and punishing the offenders. However, we experience a rebirth of shaming as norms enforcement tool. On the one side shaming is amplified through mass media in the name of crime control and entertainment [Kohm 2009] and on the other side the State reintroduces shaming no more or –at least – not primarily as punishment of sin but mainly as a tool of law enforcement and protection of the public.

---

1 Shame is a highly individualized experience that strikes at the core of a person's self-concept. About shame and shaming more analytically in Nussbaum (2004) and Ivancevich et al. (2008).

2 For example Romans branded the Latin equivalent of M for murder or V for vagrancy. See Solove (p. 91).

3 The *Hexabiblos* formed the basis of the civil law of the Greeks not only during the period of Turkish rule but also in the modern Greek state until the new Civil Code was put in force (1946).

4 In colonial America offenders of certain customs were branded or locked in pillories.

5 A powerful illustration of shaming punishment in colonial America is provided in the novel of N. Hawthorne The Scarlet Letter (1850).

In the following section (2) we discuss naming and shaming as expression of moral disapproval and integral part of crime deterrence policies. This section focuses on the examples of shaming through publicly naming of persons, who are suspects and/or convicted of crime or tax evasion in Greece. In the same section we present also the relationship between the reappearance of shaming punishments and the new conception of law enforcement and safety/security. Section 3 then presents the impacts of naming and shaming policies on the reputation as well as on the right to informational privacy and dignity of the person affected. Emphasis is given to issues concerning the impacts of shaming on the right to presumption of innocence. This section addresses also the effects of online shaming publicity, the wide availability and the persistency of information on the main principles of data protection and the rights of individuals, like the right to oblivion. In the last section (4) we assess the compliance of shaming policies with the imperatives of the proportionality principle. The first part deals with the question if shaming is appropriate, necessary and reasonable in order to achieve deterrent or rehabilitating effects. The main conclusion of this contribution is that the main problem with naming and shaming practices and measures is that they threaten the dignity of the person by making her an instrument of the State.

2. SHAMING AS SANCTION POLICY

2.1. Shaming Policies

During the last decades the so called naming and shaming strategies have been proposed especially as part of moral disapproval and crime deterrence policies. Press releases or public notices concerning incidents have long been a practice of law enforcement authorities. However, public disclosure becomes systematic and detailed [van Erp 2008]. By naming the offender a state agency condemns her in full view of the society for engaging in an unlawful and repugnant act [Blank 2009]. Shame punishments mark the wrongdoer with a degraded identity. Offenders are made to feel guilt and remorse for their acts in an effort to build consciousness und an understanding of lawfulness. Moreover the State expects the community to participate to the punishment process by disgracing and degrading the offender.

A main objective of public condemnation and social demotion of the offender is to discourage the shamed or others from committing crime in the future time [Ivancevich et al. 2008]. The main assumption is that naming publicly the offender deters others, who become aware of the incident of shaming and wish to avoid shame [Pawson 2001]. Crime deterrence theorists suggest that the «offender fears the look in the eyes of his or her intimates, including family, friends, and colleagues, who know about his behaviour, more than he or she fears punishment»[6]. In this context, shaming amounts to a formal tactic of punishment itself rather than an unintentional byproduct or outcome [Pratt 2000].

6 Ivancevich et al. p. 407.

The media, often in close collaboration with governmental agencies, take a considerable part in naming and shaming processes by publicizing reports on law enforcement actions, arrests and trials against sex offenders, paedophiles and tax evaders. In the rise of infotainment, shame penalties have become increasingly commodified [Kohm 2009][7], especially if celebrities[8] are involved in[9]. The media industry capitalizes on the public's insatiable hunger for sensations. Media seems to be the easiest way to reach the wide and appropriate public in order to achieve the specific goals of shaming. The mediatisation of reality has become so dominant that we are witnessing a transformation of what we understand as public sphere and participation to public discourse. In reporting on offenses and punishment, media signal implicitly social values [Branham 2009], while having significant effects on the popular sense of «justice for all» [Levi 2010], even if media coverage provokes often a vigilant justice.

2.2. Naming suspects and convicted sex offenders

In 2007, the Greek Parliament in response to public anger after the rape of a 9 years old girl by a man already once convicted for rape, has enacted an amendment of the Data Protection Law[10], which provided that the competent Public Prosecutor is entitled to allow the publication of the names of persons involved in criminal charges or convictions. According to the law[11], «[t]he publication of criminal charges or convictions aims at the protection of the community, of minors and of vulnerable or disadvantaged groups, as well as at the facilitation of the punishment of those offences by the State». The Minister of Justice defended the public disclosure of the names of suspects and convicted persons by arguing that this provision «throws off the masks of murders, rapists and paedophiles and all persons, who we meet in everyday life without having the possibility to handle them in the way they deserve»[12]. Not only ordinary people but also public officials and judges felt that sex offenders lost their ability to argue their civil rights and liberties when they committed such an offense[13].

---

7 Infotainment, defined as the combination or the blurring of information and entertainment, structures in a powerful way public stories about crime and crime control.

8 Some argue however that the visibility of celebrities can be used to the shaming's efficiency advantage. See Blank (2011).

9 It is noteworthy that the Council of Europe Recommendation (2003) 13 prohibits (Principle 7) the exploitation of information about ongoing criminal proceedings «for commercial purposes or purposes other than those relevant to the enforcement of the law».

10 Law 2472/97 on the protection of personal data. Available at www.dpa.gr

11 The fact that it was a hasty and improptu political response to public pressure is obvious as the respective provision is laid down as an addition to the definition of «sensitive data» (art. 2b) and not as a rule allowing the processing of this category of data (art. 7).

12 Greek Parliament, Archives of the Parliamentary Session of 13/12/07, p. 2579.

13 Some months before the Prosecutor of the Highest Civil Court pronounced in his Opinion 14/07 that the criminal behaviour of a person does not fall under the notion of personal data and their protection.

The aim of this policy is apparently multifold. Proponents of shaming policies point to the (legitimate) public safety reasons: public disclosure of the offenders' names is introduced to enable the public to protect itself from the danger posed by sex offenders[14]. The respective legislation was enacted in the heat of the moment to face what many proclaimed to be a high rate of recidivism by sexual offenders [Corenti 2010][15] however without using any study or testimony from experts. The publicity decision might also serve gathering additional evidence. Especially the naming of arrestees and/or suspects might reveal additional criminal charges, additional complainants or defendants more and –in any case – additional witnesses [Reza 2005].

2.3. Naming and Shaming Tax evaders

The naming of tax evaders is laid down as an obligation of tax authorities. Law 3843/2011 serves as the legal basis for the public disclosure of the names of the persons with debts of more than 150,000 Euros owed to the Greek State[16]. Under the pressure of the economically critical situation in Greece, a debt-laden country, State authorities concentrate their efforts on improving tax collection and controlling tax evasion. Indeed, tax evaders' naming was also conceived as tax collection means. The fear of social stigma and impacts on business should force debtors to pay their debts and discourage taxpayers from evading taxes.

In addition to enhancing deterrence, the publicity strategy aimed at increasing confidence among compliant individual taxpayers, who pay considerable attention to reciprocity[17] and fairness in relation to compliance to their tax duties. It was hoped that taxpayers and debtors would comply with their obligations and civic duties not only because they fear criminal sanctions but driven of social shaming that the public disclosure would create. The principle of tax equality and justice is embedded in the Greek Constitution[18]. At the end of January 2012, the Ministry of Finance has published a list of 4,152 debtors, after having required clearance by the Greek Data Protection Authority. The DPA approved the

14 Reza defines this «right» as «*informed living*.», i.e. the government should arguably inform the public about its suspicions regarding an arrestee or suspect so that people may practice «informed living», the right to exercise an informed choice about those with whom they live and associate.

15 The recidivism argument is widely shared and seems to be a decisive one. The U.S. Supreme Court referred (in McKune v. Lile) explicitly to the «frightening and high risk of recidivism of the offenders who refused treatment».

16 It is noteworthy that the OECD in its Report concerning Greece (2011) proposed that «the thresholds for naming evaders (€150 000) could be lowered and made systematic rather than discretionary, as seems currently to be preferred».

17 According to reciprocity theory, these types of taxpayers will comply with the tax system only if they believe that other taxpayers are paying their taxes honestly. See Blank (2011), p. 8.

18 According to article 4, paragraph 1 of the Constitution of Greece all Greeks are equal before the law and according to article 4 paragraph 5 Greek citizens contribute without distinctions to public charges in proportion to their means. The Constitution provides both the tax obligation of everyone and the guarantee of (proportional) tax equality and justice.

publication, while imposing some restrictions and exceptions[19]. It seems that the financial situation and the fight against tax evasion has been the decisive criterion for the DPA, which adopted the argumentation of the Ministry that the naming of debtors would enhance the «tax morale» and the compliance with the «civic duty» of Greeks tax payers and convey (a sense of) justice to honest taxpayers. In this socio-economical context the DPA refrained from assessing the proportionality (and especially the necessity) of the measure[20] in relation to the purposes to be achieved.

2.4. Shaming in the context of new security perceptions

Naming and shaming measures are adopted to degrade the offenders in public while inviting the public to participate to the punishment of the wrongdoers. The come-back of such scarlet-letter punishments indicates the recognition of the limited dissuasive force and the barriers of the traditional sanctions. Furthermore it reflects a shift in the conception of law enforcement and safety/security. With an important, «traditional» role of the state being the protection of the physical security of people and property, security is privileged over values such as privacy and autonomy in various strands of political philosophy [Mitrou 2010]. The contemporary politics of security and crime control focus on public protection, risk management and prevention. Managing the persons perceived to be a threat to society has become recently an acute popular and governmental concern.

Explicit appeal to shame and humiliation appears to emerge out of the popular punitivism toward a new law and order concept [Thomas 2004]. As Kohm underlines, the new law and order orientation, which became obvious at the last decades, has been a fertile ground for these new forms of punishment to be imposed by the public and via the mass media [Kohm 2009]. Naming and shaming measures implicate the society in law enforcement and crime and/or offenses punishment. The social model of collective security, dominant during the 20th century, has been slowly supplemented –and in some fields replaced– by the responsibilization of the individuals as agents of law enforcement. The community[21] is encouraged to become actively involved[22] in reporting crime, stigmatizing and imposing limitations on the offenders' freedom, chances and choices. Shaming penalties not only focus on deterrence

19 Data Protection Authority, Opinion 4/2011. Available at www.dpa.gr

20 The list did not include the names of those who have already made arrangements to settle their tax arrears. The release of the list follows months of warnings that the names would be made public. According to the press reporting many of the over 4,000 people featured in the list who owed Greece about 15 billion Euros in total, could not pay or they were/are already in prison. Topping the list with arrears of 952 million Euros is a convicted tax fraud who is already serving a 504-year prison sentence for issuing fake receipts to companies that wanted to lower their tax bill!

21 Nussbaum (p. 175) points out that communitarian political thinkers, like Etzioni, recommend the revival of shaming as a way of expressing and reinforcing shared moral values.

22 Rose (p. 324) is charactering these strategies as «ethopolitical», as they are operating through the self-steering forces of honour and shame, or propriety, obligation, trust, fidelity and commitment to others.

but they aim at or they result to an ever widening attempt to put more people under social control [Nussbaum 2004].

3. IMPACT OF SHAMING (S)A(N)CTIONS

3.1. Impact of shaming on reputation, privacy and dignity

Beyond the shame effect that a public disclosure and dissemination of information is expected to have on involved individuals, shaming might result in «sanctions» that are imposed on offenders by the (social or professional) community. The fact that a person is depicted in public as suspect or offender may strongly injure her social dignity, her reputation[23]. Public disclosure of shaming facts or suspicions affects not only the ability of a person to formulate conceptions of self, values, preferences, goals. A lost or damaged reputation may have serious impact on the ability of a person to engage in society. As everyone depends upon others and their perceptions to engage in social or professional transactions, shaming publicity threatens –often irrevocably– relationships[24], social status, current and future employment of the shamed person.

Losing control over one's own reputation is the inevitable effect of losing control over the circulation of one's own information[25]. The spread of information caused by public disclosure of the implication with a crime or an offense interferes with the right to informational privacy, which is understood both as a right to seclusion and anonymity and as prerequisite for taking autonomous decisions, freely communicating with other persons and being included in a participation society. Informational privacy is strictly related to the protection of life choices and life chances from public control and social disgrace. If public authorities and consequently the media disclose and disseminate information about the identity of a convicted or suspected person, freedom of expression[26] collides with the individual's right to privacy and anonymity[27]. Evaders, arrestees and suspects should not be deprived of their

23 D. Solove (p. 30) defines «reputation» as the «shared, or collective, perception of a person».

24 Relationships of the shamed person are affected in multiple ways: Family members are the «collateral damages» of shaming punishments. Furthermore the shamed person experiences fear, remorse and anxiety if relatives and friends abandon or isolate her because of the shaming publicity (Ivancevich et al. 2008).

25 The right to informational self-determination consists in the right of a person to know which of the information about her is known to her environment and to -principally -determine when, how, and to what extent information about her is communicated to others and used by them.

26 Which includes also the right to impart and receive information. See Art. 10 of ECHR.

27 The person's right to avoid disclosure of facts and information about her status of being accused or convicted is laid down in central european law either as confidentiality/ secrecy of the pre-trial stage or as restricted and exceptional access to criminal records. In USA the Supreme Court has repeatedly resticted access to arrest records as a consequence of the right to avoid disclosure to personal matters (Reza p. 761).

rights. On the contrary: «the more publicly embarrassing the crime, the stronger the deterrent effect – and the greater harm – of being named in connection with it»[28]. Due to the plethora of harms that attend being named and shamed as suspect or accused, the need for protection is arguably more pressing.

Undoubtly, the right to informational privacy is not an absolute one. Informational privacy may be restricted either for reasons of public interest such as security reasons or for preserving others' rights and liberties. In some jurisdictions revealing a suspect's or offender's identity is per se an issue of public interest and consequently free speech overrides the person's right to anonymity. Continental legal systems cope with the underlying conflict between freedom of information and rights to informational privacy through a process of balance of interests, either in abstracto through a legal norm or in concreto through the judging of a case by the courts[29]. Decisive are the criteria of the nature and the gravity of crime/offence, the status of the person accused or convicted, the value of the evidence (to be) gathered. Another element of crucial importance for balancing the competing rights and interests is assessing the proportionality of the harm caused to individual by the disclosure of such information in relation to the purpose to be achieved.

The claim for (protection of) privacy may not waive the accountability of a person for her actions and acts. On the other side, our (traditional?) justice system penalizes the act and is based on the conviction of a person for the crime committed. The feature and personality of the offender is of importance only for understanding and/or proving the act and for determining the concrete sanction[30]. The public disclosure of the name of a person accused or convicted for a crime aims per se at degrading and humiliating her as person. Humiliation constitutes an interference with personality of the accused and/or convicted person. Moreover, it threats her human dignity[31]. Shaming per se subjects the person to a form of peculiar vulnerability, which may deprive her of personhood and dignity [Whitman, 1998].

3.2. Shaming and presumption of innocence

Reputation, privacy and dignity are not the only interests and values that are infringed by naming and shaming actions. Affected may be also the so-called presumption of innocence, which is understood as the right to be presumed innocent until the conviction. In some jurisdictions the presumption of innocence is meant as an evidentiary rule without acknowledging

28 Reza, p. 773.

29 About the ECHR case law in relation to Art. 10 see Council of Europe, Freedom of Expression in Europe (2007).

30 For example the Greek Penal Code , which reflects the central-European tendencies in penal law, provides (Art. 68) for the publication of a penal judgment only on the basis of a ruling of the Court to be made either ex officio for reasons of public interest or following a request of the victim who has a legitimate interest.

31 Nussbaum (p. 230) argues that when the public laughs at someone in the pillory, people are not invited to focus on the committed criminal or unsocial act.

any application or effect before trial. In Europe the presumption of innocence conditions the treatment of an accused person throughout the phase of criminal investigations up to the end of trial[32]. According to the European Court of Human Rights, from Article 6 § 2 of the ECHR is also drawn that every person has the right not to be publicly presented as offender before final conviction. Recognizing this right only as an instrument of proof would result in legitimizing the humiliation imposed upon persons accused but not yet convicted on crime.

Art 6 § 2 of the Convention binds not only judges or courts but also any other public authority. Recently, this principle is applied also to the horizontal relationships between privates. Presumption of innocence is becoming a «normative parameter» in the balancing of rights of the affected persons and the informing media. The Council of Europe Recommendation (2003) 13 on the provision of information through the media in relation to criminal proceedings provides(Principle 10) that «in the context of criminal proceedings, particularly those involving juries or lay judges, judicial authorities and police services should abstain from publicly providing information which bears a risk of substantial prejudice to the fairness of the proceedings». This approach should prevent shaming punishments at least prior to conviction and especially at a time when the words «suspect» and «offender» are becoming increasingly synonymous [Quintard-Morenas 2010].

3.3. Impact of shaming in digital age

The impact of shaming on the affected persons cannot be assessed without taken into account the techno-social context of shaming actions. The rise of Internet[33] and the exponential increase of its content, its possibilities and its actors/users opened up a vast frontier for shaming and humiliating individuals. Accessing and gathering information on offenders and offenses has become ease, cheap and routine. The shift to online media, the ability to search newly digitized collections of information (such as old newspapers), the fact that many courts make their records available means that past information is more accessible than ever before [Solove 2007, Schwartz 2009].

There is virtually no limit to the amount of information that can be recorded and to the time period that it can be stored. The persistency of information entails that it can last longer than the circle and context, in which its processing was legitimate. The online availability and accessibility of information that was legally published offline in the past is not at all self-evident. In connection with the wide availability this persistency undermines the principles of purpose limitation and proportionality[34] or the rights of individuals, like the

32 France (French Code Civil, Art. 9-1) has reinforced the presumption of innocence by providing it as a personality right.

33 Naming and shaming of offenders could take place through traditional media but now reports about offenses can be published on the Internet without any cost or effort. More analytically see Meijer et al. 2009.

34 According to the U.S. Supreme Court, «...notice of a criminal conviction subjects the offender to public shame, the humiliation iucreasing in proportion to the extent of publicity» (Case Smith v. Doe).

right to oblivion[35], i.e. the right to forget and to be forgotten [Mitrou 2010][36]. Moreover, information stored and accessed on the Web consists of fragments of people's lives that may be out of context, at random, incomplete or wrong [Solove 2007]. This is especially the case where a suspect has been acquitted of all the charges. Having been accused of a crime lasts in the public eye, although vast numbers of arrestees are dismissed soon after arrest, and countless accusations are unfounded or improvable. Rarely acquittal or dismissal of charges receives as much public attention as arrest or suspicion. Even if information is corrected on the source websites, Internet archives, cache copies and various abstracts produced by search engines may still provide an inaccurate and distorted status/picture of the person[37].

The ubiquity of data collection practices, advances in search methods, content creation, decreasing costs of infinite storage enhance perpetual dissemination of shaming information and threaten to erode what we understand as social forgetting [Ambrose et al. 2011]. In the «global village» shaming is no more a temporary mark of disgrace and becomes a widespread and lasting inscription of stigma [Solove 2007]. Due to the Internet's perfect and perpetual memory it is becoming harder and harder for people to escape their past[38]. Some years ago (2009), Wikipedia has been sued by two Germans who claimed that the online encyclopaedia's description of their involvement in the murder of a German actor back in 1990 violates their right to privacy. They had already successfully pressured German publications to remove their names from their online coverage[39]. German editors of Wikipedia had scrubbed their names from the German-language version of the article about the victim, the actor Walter Sedlmayr. By supporting their right to privacy after having «paid their debt to society» their lawyer underlined that «they should be able to go on and be resocialized, and lead a life without being publicly stigmatized»[40].

35 Bernal (2011) refers to the right to oblivion as a right to silence on past events in life that are no longer occuring, such as crimes for which the person has been exonerated.

36 Due to the enormous risks associated with the proclaimed total and eternal memory of the Internet, the right to oblivion has been proposed as an explicit right to be enshrined in the EU (Draft) General Data Protection Regulation. Available at http://ec.europa.eu/justice/data-protection/document/review2012/

37 In Greece a person, accused and acquitted of all charges, sued a newspaper claiming to remove the respective information from its website. The newspaper proved that it had no more the technical possibility to remove the inaccurate content, because it was actually saved on a mirror page. On January 2006, the Italian Garante Privacy has called upon Google to find out solutions to remove obsolete or inaccurate personal information after such information has been amended at the source websites. See Liguori and De Santis, The Right to be Forgotten: Privacy and online News (18/3/2011), available at www.portolano.it

38 As expressed by the EU Commissioner Viviane Reding »God forgives and forgets, but the Web never does».

39 The Swedish Data Inspectorate had decided that five years after the information has been published , the only key to sensitive data to be used for search to electronic archives should be the date of publication and not the name of suspect or convicted person (Council of Europe, 1990).

40 Report of November, 12 (2009) in The New York Times online edition. Available at ttp://www.nytimes.com/2009/11/13/

4. CONCLUSION

4.1. Is shaming appropriate, necessary and/or efficient?

In the age of «perfect» or «excessive» remembering[41] perpetual memory has a devastating impact: it hinders forgetting and decreases the chances of forgiveness. Thereby, the persistence of shaming information limits the ability of a person to pursue in life and to change it. Through the right to oblivion forgiveness is tied to privacy and the ability to escape the past and build the future. Besides, imposing sanctions aims both to deterrent crime and to rehabilitate the offender, allowing her the re-integration into society.

An issue meriting discussion is the appropriateness, the necessity[42] and the stricto sensu proportionality of shaming punishment in relation to the purposes to be achieved. The right to privacy as well as the more specific right to be forgotten should be carefully shaped in order to strike an adequate balance between this right and other important rights and interests, such as freedom of speech and information or law enforcement purposes. Lawfulness and acceptance of applying shaming measures on suspects and convicted offenders depends on whether evidence can be presented that this form of incidental sanctions are necessary, effective, efficient and fair. The driving forces behind publicity of offenders' identity are to prevent re-offense and to appease the anger of the public. Does branding these people insure public safety or provide a false sense of security? Does shaming effectively deter crime or change people's views and values about compliance with the law and harmfulness of criminal behaviour or tax evasion? These questions should be addressed by empirical research. Actually there is no statistical or practical evidence that shaming is appropriate, necessary and reasonable in order to achieve deterrent or rehabilitating effects.

In the case of sex offenders there are several studies that question the efficiency of naming and shaming strategies. There are serious doubts on the effectiveness of sex offender registries (as provided for example by Megan Laws in USA) to significantly reduce rates of sexual offending [Corenti 2010]. Furthermore scholarly research does not support that sex offenders will repeatedly re-offend and the vast majority of child victims are victimized at the hands of relatives, acquaintances or family's friends [Kohm 2009]. As far as it concerns types of extreme offenders it is unlikely that shaming actions would lead them to change their behaviour in response to the fear of humiliation and stigma [Owens 2001].

Shaming is pertinent to persons accused or convicted of tax evasion. However, it is highly questionable if shaming publicity may play a significant role in determining compliance with the law [Murphy and Harris 2007]. What is shown by studies is that tax enforce-

41 About the analysis of forgetting and forgetfulness see Mayer-Schönberger, who characterizes forgetting as «a life-saving advantage».

42 According to the jurisprudence of the ECHR on Art. 8 § 2 of the Convention, restrictions of privacy rights have to pass the so-called «democracy test»: even if a restriction is foreseen in law and serves a public interest, it (the restriction) has still to be necessary in a democratic society and shouldn't reach further than what is strictly necessary.

ment actions against offending taxpayers and especially actions that involve penal sanctions may have an important and positive deterrence effect [Blank, 2011]. Moreover, studies have shown that choices about compliance are influenced by multiple factors, while research has also revealed that deterrence-based enforcement strategies sometimes generate future resistance to compliance with tax law [Murphy and Harris 2007].

To deter persons from engaging in unlawful behaviour, shaming sanctions must threaten to harm their reputations within their communities. Furthermore, the deterrence effect of shaming actions depends upon the relationship of the person affected by shaming to her community, on the networks of mutual social understandings in society as well as upon the values and attitudes of the latter. It is argued that wide-ranging use of shaming sanctions is likely to erode their effectiveness, and that their extensive use especially as a substitute for traditional law enforcement actions may undermine their deterrent effects [Harel and Klement 2005]. Some authors point out the necessity of re-integrating procedures, which are important to prevent shaming from devolving into pure vigilantism.

4.2. Some concluding remarks

The power of shaming actions to deter crime and to rehabilitate the criminals seems to be questionable. Shaming measures frustrate the primary purpose of justice, i.e. to reintegrate the wrongdoer into society [Solove 2007]. Punishment should aim at and end in connecting the offender and the society to an understanding of lawfulness by internalizing lawful values. Shaming signalizes a moral condemnation of the offending conduct. However, shaming publicity is primarily conceived and designed to humiliate the offenders while inviting the public to participate to their punishment by disassociating from them or even ostracizing them into a permanent «underclass».

In naming and shaming the State metes out sanctions through its own established and legitimized institutions. Law enforcement or justice by shaming means is not the impartial, neutral justice that is typically expected by a liberal-democratic state and society. Moreover, shaming measures are unreliable as they may target persons who will be acquitted of any charge. Furthermore, such measures are difficult to balance: in many cases the impact on offenders may be disproportional to the severity of the offense [Solove 2007].

Virtually, every person convicted for serious crimes suffers humiliation and shame simply in virtue of being punished[43]. Shaming publicity destructs a person's reputation and dignity, regardless of the fact that this person actually feels humiliated or not. Crime and offense is not a sufficient reason to treat people without due respect. A democratic, liberal state does not simply respect the dignity of those who obey the law, but of all people. Shaming as intended consequence and/or true end is not consistent with the values of a democratic state. Individuals remain accountable over time for the consequences of their acts and behaviour but both shaming and persistent digital remembering foreclose the opportunity for the of-

43 U.S. Supreme Court in Case U.S. v. Koon.

fender to redefine herself and to be recognized as having the basic dignity of moral agency [Kahan 2006].

Dignity, an intrinsic value in each human being, requires the State to recognize and respect it for the welfare of the individual and not the reverse [Cheyng 2012]. Even if naming and shaming serves deterring crime, a goal of public interest, shaming constitutes an interference with ethical and psychological integrity of a person. Even if indirectly, offenders are used for display purposes. The shamed offender is used as an instrument of the state, as means and not as end. A decent society, moreover a democratic, liberal State should built on norms of respect and protect its citizens from degradation and humiliation.

5. BIBLIOGRAPHY

Ambrose M., Friess N., Van Matre J. (2012). Seeking Digital Redemption: The Future of Forgiveness in the Internet Age. Pages 1-55. Retrieved from work.bepress.com

Bernal, P. (2011). A Right to Delete? European Journal of Law and Technology, Vol. 2 (2). Retrieved from http://ejlt.org/article/view/75/144

Blank J. (2009). What's Wrong With Shaming Corporate Tax Abuse, Tax Law Review Vol. 62:541-592

Blank, J. (2011). In Defense of Individual Tax Privacy. New York University Law and Economics Working Papers. Paper 263. Retrieved from http://lsr.nellco.org/nyu_lewp/263

Branham E. (2009). Closing the Tax Gap: Encouraging Voluntary Compliance through Mass-Media Publication of High-Profile Tax Issues. Hastings Law Journal Vol. 60: 1507-1533

Cheung A (2012),Revisiting Privacy and Dignity: Online Shaming in the Global E-Village. Retrieved from http://ssrn.com/abstract=2010438 or http://dx.doi.org/10.2139/ssrn.2010438

Corenti A. (2010). The new Scarlet Letter: Twenty years of Megan's Law and a study of its history and impact on America (Thesis). Retrieved from http://gradworks.umi.com/14/90/1490134.html

Council of Europe (1990). Data Protection and Media – Study prepared by the Committee of Experts on Data Protection. Strasbourg

Council of Europe (2007), Freedom of Expression in Europe – Case Law. Strasbourg

Harel A. and Klement A. (2005). The Economics of Shame: Why More Shaming May Deter Less, Tel Aviv University Law & Econ. Workshop The Interdisciplinary Center Law & Econ. Workshop15-16 (August 24, 2005). Retrieved from http://ssrn.com/abstract=789244).

Ivancevich J., Konopaske R. and Gilbert J. (2008). Formally shaming white-collar criminals. Business Horizons 51: 401-410

Kahan D.(2006). What's Really Wrong with Shaming Sanctions. (*Faculty Scholarship Series).* Paper 102.

Retrieved from http://digitalcommons.law.yale.edu/fss_papers/102

Kohm S. *(2009). Naming, shaming and criminal justice:Mass-mediated humiliation asentertainment and punishment. Crime Media Culture* 5. pp. 188-205

Levi, M. (2010), Serious tax fraud and noncompliance. Criminology & Public Policy, 9: 493–513

Mayer-Schönberger V. (2009). DELETE: The Virtue of Forgetting in the Digital Age. Princeton: Princeton University Press.

Meijer, A., Burger, N. and Ebbers, W. (2009). Citizens4Citizens: Mapping Participatory Practices on the Internet. *Electronic Journal of e-Government* Vol. 7 (1) :99 - 112

Mitrou L. (2010). Privacy challenges and perspectives in Europe. In M. Bottis (ed.), An Information Law for the 21st Century (pp. 220-236). Athens: Nomiki Vivliothiki.

Murphy K. and Harris N. (2007). Shaming, Shame and recidivism, British Journal of Criminology 47: 900 – 917

Nussbaum M. (2004). Hiding from Humanity – Disgust, Shame and the Law. Princeton and Oxford : Princeton University Press

Owens J. (2001). Have we no Shame?: Thoughts on Shaming, «White Collar» Criminals, and the Federal Sentencing Guidelines . American University Law review (Vol. 49): 1047-1058

Pawson R. (2001). Evidence and Policy and Naming and Shaming. ESRC UK Centre for Evidence Based Policy and Practice: Working Paper 5.

Pratt, J. (2000). Emotive and Ostentatious Punishment: Its Decline and Resurgence in Modern Society, Punishment & Society 2(4): 417–439

Quintard-Morenas F. (2010). The Presumption of Innocence in the French and Anglo-American Legal Traditions, The American Journal of Comparative Law, Vol. 58: 107 -150

Reza S. (2005). Privacy and the criminal arrestee or suspect: in search of a right, in need of a rule. Maryland Law Review 64: 755-874

Rose N. (2000), Government and control. British Journal of Criminology 40: 321 -339

Schwartz P. (2009). From Victorian Secrets to Cyberpace Shaming. University of Chicago Law Review 76, pp 1407-1448

Solove D. (2007). The Future of Reputation – Gossip, Rumor and Privacy on the Internet. New Haven and London: Yale University Press

Thomas T. (2004) . When public protection becomes punishment? The UK use of civil measures to contain the sex offender .European Journal on Criminal Policy and Research 10: 337–351

van Erp J. (2008). Reputational Sanctions in Private and Public Regulation. *Erasmus Law Review* Vol. 1 Issue 5, pp. 145-162

Whitman Q. (1998). *What is Wrong with Inflicting Shame Sanctions?* Yale Law Journal 107 : 1055-1092

EL PODER DE AUTODETERMINACIÓN DE LOS DATOS PERSONALES EN INTERNET

Mª Dolores Palacios González
Profesora Titular de Derecho civil; Universidad de Oviedo

RESUMEN: La determinación del contenido y extensión de la protección de datos en Europa se encuentra en un momento de inflexión. Como consecuencia del recurso presentado ante la Audiencia Nacional por sociedades del grupo Google frente a varias resoluciones de la Agencia Española de Protección de Datos, en las que se obliga al buscador a eliminar la posibilidad de acceder a los relativos a los reclamantes, se ha presentado una cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea planteando, entre otros interrogantes, si un buscador puede ser responsable del tratamiento de datos personales. A su vez, la Comisión acaba de proponer una modificación de la legislación de protección de datos con especial preocupación por Internet y, más en concreto, por las redes sociales, con el fin, entre otros, de establecer el llamado «derecho al olvido», que en el ámbito de la red no se configura como un poder absoluto de los titulares de datos personales para eliminarlos cuando quieran y sin condiciones sino como una referencia unitaria al ejercicio de las facultades de revocación del consentimiento, oposición y cancelación, ya recogidas en la legislación de protección de datos, frente a los responsables del tratamiento digital.

PALABRAS CLAVE: Internet; privacidad; libertad de expresión; libertad de información; protección de datos: consentimiento, revocación, oposición, cancelación; publicidad comportamental; redes sociales; derecho al olvido.

1. INTRODUCCIÓN

A pesar de la trascendencia de la cuestión, actualmente es difícil determinar cómo y hasta dónde se puede proteger la privacidad en Internet, teniendo además en cuenta el juego de otros intereses como las libertades de expresión e información o incluso la libertad de empresa, incluida la de las que ofrecen servicios de la sociedad de la información. Mientras los Estados y los organismos supranacionales estudian y establecen medidas de todo orden para intentar salvaguardar los derechos de los ciudadanos frente a vulneraciones de su privacidad, en la actuación de las entidades que operan en la red se observan actitudes contradictorias. Por un lado, efectivamente mejoran los mecanismos para el control de sus datos personales por los usuarios pero, por otro, instauran procedimientos técnicos que generan más riesgos para la protección de esos mismos datos.

En el ámbito de la Unión Europea hay en este momento dos cuestiones abiertas que afectan especialmente a nuestro país. Por una parte y como consecuencia de los recursos presentados ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional por sociedades del grupo Google frente varias resoluciones de la Agencia Española de Protec-

ción de Datos en las que se obliga al buscador a eliminar la posibilidad de acceder a los relativos a los reclamantes, se ha presentado una cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea. A su vez, esta última acaba de proponer una modificación de la legislación de protección de datos con especial preocupación por Internet y, más en concreto, por las redes sociales, con el fin, entre otros, de establecer el llamado «derecho al olvido».

2. LA ACTUAL SITUACIÓN JURÍDICA DE LA PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA

Desde un punto de vista jurídico el punto de partida de la protección de datos personales es el artículo 16 del TFUE teniendo en cuenta, además, que desde el año 2000 la privacidad y la protección de datos personales están recogidos en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, lo que indudablemente afecta al alcance de la competencia de la Unión. Por supuesto, esto no implica olvidar la trascendencia de otros derechos como las libertades de expresión e información o la libertad de empresa, recogidos en los artículos 11 y 16 de la Carta, respectivamente.

Como intento de culminación del proceso de revisión del acervo comunitario en materia de protección de datos la Comisión ha decidido promover la aprobación de un Reglamento sustitutivo de la Directiva 95/46 CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales con el fin de hacerla más efectiva[1]. El marco jurídico se completará, en su caso, con una Directiva que remplazará la decisión marco 2008/977/JAI, en relación con las reglas relativas a la protección de datos de carácter personal tratados con fines de prevención y detección de infracciones penales, de las investigaciones y procesos sobre la materia, así como de actividades judiciales conexas.

Entre los diversos principios en que se basa la Propuesta de Reglamento, resulta especialmente relevante en relación con los concretos temas que se van a tratar aquí, que los datos recogidos para finalidades determinadas, explícitas y legítimas no puedan ser tratados posteriormente de manera incompatible con esas finalidades, también la adecuación, pertinencia y limitación de los datos tratados a lo necesario teniendo en cuenta los fines del tratamiento, y la conservación de los datos de forma que permitan la identificación del interesado durante el tiempo que no exceda del necesario para la realización de los fines para los que son recogidos, de tal manera que solo podrán ser conservados durante más tiempo en la medida en que no sean tratados más que a fines de investigación histórica, estadística o científica de acuerdo con una serie de reglas y condiciones establecidas en el Reglamento y procediendo a un examen periódico con el fin de valorar la necesidad de continuar conservándolos.

1 COM (2012) 11 final (http: www.eur-lex.europa.eu).

3. DATOS PERSONALES Y RESPONSABLE DEL TRATAMIENTO

Uno de los problemas que la realidad de la práctica está poniendo de manifiesto es la necesidad de concretar exactamente a qué nos referimos cuando hablamos de datos personales como objeto de protección. Tanto en la Directiva 95/46/CE como en la Ley española de protección de datos (Ley Orgánica 15/1999), el concepto de dato personal de una persona física se hace depender de la identificabilidad de aquella, como cualquier información concerniente a personas físicas identificadas o identificables. Lo que no queda bien determinado es si la identificabilidad exige siempre la posibilidad de conocer su nombre o, como se ha señalado, se produce también en relación con datos que sin identificarla en sentido estricto permiten individualizarla para tomar decisiones con respecto a ella[2].

En este sentido la Agencia Española de Protección de datos española ha defendido que debería establecerse un concepto de dato personal que cubra las situaciones en las que se desconoce el nombre del sujeto pero se tiene un perfil completo sobre él[3]. Esta amplitud se reconoce también por el Grupo de Trabajo del artículo 29, incluyendo las cookies y las direcciones IP[4].

Frente a una concepción amplia que lleve a la posibilidad de considerar que existe identificación cuando se puede tomar una decisión con respecto a una persona aunque no esté individualizada o no sea individualizable (el caso de que a partir de cookies las empresas puedan dirigir la publicidad que envían a partir del perfil generado) existen opiniones que entienden que la extensión no respeta la definición de la Directiva y que, además, plantea problemas a la hora de ejercer el derecho de acceso pues la persona a la que se refiere una cookie, que no está identificada, tendrá que identificarse para poder acceder a los datos generados[5]. La argumentación no es baladí y además en todo caso hay que tener en cuenta que el Considerando 26 de la Directiva, cuanto menos norma de alcance interpretativo en relación con el articulado, dice que para determinar si una persona es identificable hay que considerar el conjunto de medios que pueden ser razonablemente

2 Cfr. Lolin, C. y Poullet, U. (2011). Sociedad de la información y marketing: case study (traducción de María Rosa Llácer Matacás) en *Protección de datos personales en la sociedad de la información y la vigilancia*, Llácer Matacás, M.R., (coord.), Madrid: La Ley, p. 239. Señalan los autores que la pregunta merece formularse en relación, por ejemplo, con los datos registrados mediante cookies que no se refieren a un individuo sino a una sesión abierta en un ordenador.

3 Vid. el Dictamen 4/2007 sobre el concepto de datos personales y también la Contribución de la Agencia Española de Protección de Datos a la Consulta de la Comisión sobre un enfoque global de la protección de datos personales en la Unión Europea.

4 Cfr. el Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda. A su vez, el Dictamen 2/2010 señala que en la medida en que la obtención de perfiles mediante cookies puede permitir la identificación, son datos personales identificables sometidos a la regulación de la Directiva 45/96. En cuanto a la AEPD véase el Informe 327/2003.

5 Cfr. Colin y Poullet, Y, cit., p. 241.

utilizados para la identificación por el responsable del tratamiento o por cualquier otra persona. Este último criterio restrictivo de la identificabilidad ha sido acogido en nuestro Derecho por el Real Decreto 1720/2007 que aprueba el Reglamento de Protección de datos, cuando en el apartado o) del artículo 5 prevé que una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados. Se trata de un criterio de proporcionalidad y razonabilidad que lleva a concluir que no son datos personales protegibles los que solo permitan individualizar a la persona utilizando medios o tiempos excepcionales o muy largos. En cuanto a la propuesta de Reglamento comunitario, aunque el artículo 4.1 define al interesado como cualquier persona física identificada o identificable, directa o indirectamente, por medios razonablemente susceptibles de ser utilizados por el responsable del tratamiento o por cualquier otra persona, en particular por referencia a un número de identificación, datos de localización, un identificador en línea o uno o más elementos específicos característicos de su identidad física, psicológica, genética, psíquica, económica, cultural o social (art. 4.1), en el Considerando 24 se dice que los números de identificación, los datos de localización, los identificadores en línea u otros factores específicos no necesariamente tienen que ser considerados datos personales en toda circunstancia.

Dejando aparte el concepto de datos personales, el problema de su protección se plantea cuando una persona ajena al titular de los mismos decide sobre su uso. Se le considera entonces responsable del tratamiento, que según la normativa de protección de datos es quien tiene disponibilidad de los recogidos en un fichero, como conjunto organizado de datos[6]. Por lo que se refiere a los recogidos en la red la Agencia Española de Protección de Datos ha considerado que tanto los sitios web como los buscadores realizan un tratamiento de datos personales y que, por tanto, están sometidos a la regulación de la Ley de Protección de Datos. Respecto a las páginas web, la Agencia se apoya en la doctrina de las Sentencias de 17 de marzo de 2006, de la Audiencia Nacional, que consideró que un sitio web requiere siempre una organización y estructura, y de 6 de noviembre de 2003, del Tribunal de Justicia de la Unión Europea, en la que se dice que «la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un tratamiento total o parcial de datos personales»[7]. En cuanto a los buscadores, veremos más adelante que también los considera responsables del tratamiento [8].

---

6 Cfr. Art. 2.c de la Directiva 95/46/CE y 3 b) de la LOPD).

7 Resolución R/00937/2010.

8 No obstante, se verá también que el Auto de la Sala de lo Contencioso Administrativo de la Audiencia Nacional de 27 de febrero de 2012 plantea al Tribunal de Justicia de la Unión Europea precisamente, entre otras cuestiones prejudiciales, si «debe interpretarse una actividad como la descrita (se refiere a la actividad propia de un buscador) comprendida en el concepto de tratamiento de datos» contenido en el art. 2.b de la Directiva 95/46/CE. La cuestión, por tanto, no está cerrada.

4. EL PRINCIPIO GENERAL DE LA DISPONIBILIDAD DE LOS DATOS POR EL INTERESADO

Como no puede ser de otra manera dada la íntima relación existente entre los datos personales, el derecho fundamental a la intimidad y, más ampliamente, la dignidad personal, la regla general para poder proceder al tratamiento de los datos de una persona es haber obtenido su consentimiento. La otra cara de la moneda de ese derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad provenientes del uso ilegítimo del tratamiento mecanizado de datos es la posibilidad evitar ese tratamiento[9]. En este sentido y según la legislación de protección de datos caben varias posibilidades: revocar el consentimiento, oponerse al mismo o ejercitar los derechos de rectificación y cancelación.

4.1. Consentimiento para el tratamiento de datos personales

De acuerdo con la Directiva 95/46 CE, la Ley Orgánica de Protección de Datos exige que el consentimiento para el tratamiento de los datos referentes a una persona ha de ser libre, inequívoco, específico e informado[10]. Por tanto, no es necesario que tenga carácter expreso en el sentido de que tenga que haber una declaración al efecto, verbal o escrita[11], sin perjuicio de que en el caso de consentimiento tácito la actuación de la que se deduzca el consentimiento resulte indubitada en este sentido. Por su parte, la propuesta de Reglamento comunitario define el consentimiento como manifestación de voluntad libre, específica, voluntaria, informada y explícita, por la que el interesado acepta por una declaración o un acto positivo inequívoco que los datos de carácter personal que le conciernen sean objeto de tratamiento. Pese a esa exigencia literal del carácter expreso del consentimiento realmente no se produce ningún cambio sustancial respecto de la regulación hoy vigente pues al preverse la posibilidad de que se deduzca de un acto positivo inequívoco, todo se reduce a una cuestión lingüística[12].

Por lo que se refiere las actuaciones dirigidas a utilizar publicidad comportamental en el marco de Internet, que se realiza mediante la actuación de los proveedores de redes de

9 Cfr. STC 292/2000 que dice expresamente que el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. Y que el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que solo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ 7).

10 Cfr. artículos 3 h., 5 y 6 de la LOPD.

11 En este sentido, Informe de la AEPD 49/2007.

12 Vid. Considerando 25 de la Propuesta de Reglamento.

publicidad, los anunciantes y los editores, y a las que les es aplicable la Directiva 95/46 en lo no regulado por la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, el artículo 5.3 de la Directiva 2002/58/CE, modificado por la Directiva 2009/136/CE, y transpuesta en nuestro ordenamiento por el Real Decreto Ley 13/2012 de 30 de marzo, exige que previamente se haya obtenido el consentimiento informado de los usuarios[13]. La información deberá ser clara y precisa y abarcar la identidad del responsable de instalar las cookies y recoger la información correspondiente, el funcionamiento de las cookies, el tipo de información que se recaba y la finalidad del tratamiento. Dicho consentimiento puede obtenerse a través de los parámetros adecuados del navegador, siempre que el usuario del ordenador reciba la información previa adecuada y suficiente y que realice una acción expresa para modificar la configuración predeterminada que por defecto rechace la recogida y tratamiento de la información para permitir así el uso de las cookies[14].

Hay casos en que los que la Ley de Protección de Datos no considera necesario el consentimiento del interesado para el tratamiento de su datos: cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado; o cuando sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado (art. 6.2 LOPD). En relación con esta última excepción, a la necesidad del interés legítimo añade el precepto «que los datos figuren en fuentes accesibles al público», pero esta exigencia ha de entenderse suprimida tras la Sentencia de la Sala Tercera del Tribunal Supremo de 8 de febrero de 2012[15].

---

13 La citada transposición ha dado lugar a una nueva redacción del artículo 22 de la Ley de Servicios de la Sociedad de la Información.

14 Esta interpretación del precepto es la que recoge el Dictamen 2/2010 del Grupo de Trabajo del artículo 29 sobre publicidad comportamental en línea.

15 Realmente esta sentencia lo que anula es el artículo 10.2 letra b) del RD 1720/2007, de 21 de diciembre, que aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, y en el que se reproduce la excepción de la LOPD, por considerar, conforme a la respuesta dada por el Tribunal de Justicia a la cuestión prejudicial planteada al efecto (Sentencia de 24 de noviembre de 2011, asuntos acumulados C-468 y 469/10), que la exigencia de que los datos figuren en fuentes accesibles al público no viene recogida en el artículo 7 letra f) de la Directiva 95/46 y que los Estados miembros no pueden imponer exigencias adicionales a las previstas en el citado artículo 7, pues modificarían el alcance de alguno de los principios establecidos en dicho artículo. El Tribunal no declara la nulidad del precepto de la LOPD que la recoge al entender que la jurisdicción contencioso-administrativa no extiende su conocimiento a disposiciones con rango de ley, pero la ineficacia de esa previsión sí anulada en el Real Decreto puede deducirse, como ha señalado Marín López, J., de la afirmación del Tribunal de Luxemburgo en el apartado 55 de la resolución mencionada de que el artículo 7 f) de la Directiva 95/46 tiene efecto directo. Vid. Marín López, J. (2012). El tratamiento de datos personales sin con-

El hecho de que, por tanto, haya de entenderse que es suficiente el interés legítimo de quien realiza el tratamiento para que sea posible sin consentimiento del interesado, sin necesidad de que los datos provengan de fuentes accesibles al público, no debería llevar a pensar que se ha producido cambio alguno respecto de la necesidad del consentimiento como principio o regla general. Por una parte, se exige que el tratamiento sea necesario para satisfacer el interés legítimo y, por otra, la no vulneración de los derechos fundamentales del titular de los datos como límite, lo que sin duda tiene una trascendencia especial teniendo en cuenta que el derecho al control de los propios datos es en sí mismo un derecho fundamental derivado de la propia dignidad de la persona. En definitiva, como señala el propio Tribunal de Luxemburgo en la sentencia de 24 de noviembre de 2011, para que los datos personales puedan efectivamente tratarse sin consentimiento del interesado será necesario, además de la existencia de un interés legítimo del responsable del tratamiento, la «ponderación de los derechos e intereses en conflicto, que dependerá, en principio de las circunstancias concretas del caso particular de que se trate y cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado» (apartado 40)[16].

Por lo que se refiere a las libertades de expresión y/o información y pese a que legislador español no se refiere expresamente a la licitud de hacer públicos datos personales en el ejercicio de las mismas ni regula directamente su ponderación con el derecho de protección de datos[17], la posibilidad de hacer públicos datos personales ajenos en legítimo ejercicio de

---

sentimiento del interesado tras la sentencia del Tribunal Supremo, Sala 3ª, de 8 de febrero de 2012, http://www.diariolaley.es, diario de 24 de febrero de 2012.

16 Señala en este sentido Marín López, J., cit., que «la STS de 8 de febrero de 2012 no puede ser entendida, como tan precipitada y erróneamente se ha dicho (y escrito), en el sentido de que el tratamiento de los datos personales no precisa ya consentimiento del interesado. Se oponen a esta conclusión no solo el artículo 10.1 del Reglamento de 2007, que no fue cuestionado en ningún momento por el recurrente, sino también los – superiores en rango jerárquico – artículos 6.1 LOPD y 7 a) Directiva 95/46. En el mismo sentido se pronuncia Martínez Martínez, R., cuando señala que el artículo 7 f) de la Directiva impone una condición: no basta con la presencia de interés legítimo pues éste cede cuando prevalezca el interés o los derechos y libertades fundamentales. Desde el punto de vista del autor el precepto obliga al responsable «a transitar por la frontera de las excepciones al consentimiento, que no es ocioso recordar al tratase de un derecho fundamental deberán interpretarse restrictivamente» y estando en juego derechos fundamentales «se impone un juicio de idoneidad de modo que no bastará con que la medida, en este caso el tratamiento, sea legítima sino idónea o adecuada al fin perseguido, un juicio de necesidad para determinar si de entre todas las posibilidades es la menos lesiva o gravosa para el derecho fundamental, y finalmente, un juicio de proporcionalidad que establezca si ofrece más ventajas para el interés general que perjuicios» (www. el derecho/con/administrativo/Interes-proteccion-personales-Tribunal-Supremo_11_372805001.htlm).

17 La Directiva 95/46 remite al ámbito interno la regulación de dicha ponderación (vid. Considerando 37 y artículo 9). A su vez La STJCE de 6 de noviembre de 2003 (caso Lindqvist), señala que la ponderación bajo el principio de proporcionalidad ha de hacerse por el juez nacional, en sede estatal. Vid. asimismo Considerando 121 y artículo 80 de la Propuesta de Reglamento sobre Protección de datos.

aquellas, sin necesidad de consentimiento, se ha fundamentado tanto directamente en el artículo 20 de la Constitución[18] como en el inciso primero del artículo 6 de la LOPD cuando señala que el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado «salvo que la ley disponga otra cosa»[19].

4.2. Revocación del consentimiento y derechos de oposición y cancelación

Conforme al apartado 3 del artículo 6 de la LOPD el consentimiento puede ser revocado siempre que exista «causa justificada» . En principio parece que en cualquier caso sería necesario alegar y probar una justificación pero esta conclusión es excesiva. Teniendo en cuenta la trascendencia del consentimiento, que la disponibilidad de los datos que, en su caso, fundamenta el mismo afecta a derechos fundamentales de la persona y que la Directiva no dice nada en relación con la revocación, solo cabe concluir que, en principio, la revocación del consentimiento ha de ser tan libre como la emisión. De hecho, el artículo 17 del Reglamento de desarrollo de la Ley, de acuerdo con esta posibilidad, establece que la revocación ha de permitirse a través de un medio sencillo y gratuito, sin ninguna condición. A su vez la propuesta de Reglamento comunitario prevé que el consentimiento del interesado podrá ser retirado en cualquier momento sin ningún condicionamiento adicional[20].

Cosa distinta es que la posibilidad de revocación sin justificación haya de ponderarse en relación con otros derechos o intereses legítimos de terceros, del propio responsable del tratamiento o incluso, con cuestiones de interés general (derecho a recibir información, interés histórico, de enseñanza, etc.). En este sentido y concretamente en relación con los derechos adquiridos en el marco de una relación contractual, lo razonable será que la revocación del consentimiento del contratante cedente quede supeditada a la indemnización de los perjuicios que se hayan podido causar al contratante cesionario.

Por su parte la oposición al tratamiento es la facultad que la ley reconoce al titular de los datos en los casos en que no es necesario su consentimiento para el tratamiento y siempre que no haya ley que se oponga a ello. También en este supuesto la LOPD exige con carácter general, en su artículo 6.4, motivos fundados y legítimos, en este caso relativos a una situación personal.

El Real Decreto 1720/2007 desarrolla el ejercicio de esta facultad, de acuerdo con los presupuestos de la Directiva del 46/95/CE, en el artículo 34. Se prevé, además de en los casos en que no es necesario el consentimiento, cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en cuyo caso

18 Arias Máiz, V. (2010) Una excepción al principio del consentimiento informado no contemplada en el artículo 6 LOPD: el uso de datos personales por medios de comunicación en *Comentario a la Ley Orgánica de protección de datos de carácter personal*, Troncoso Reigada (dir.), pp. 560 ss.

19 Lo que sí parece más discutible es que sea una autoridad administrativa, la Agencia de Protección de Datos, la competente para decidir en caso de conflicto entre derechos fundamentales.

20 Art. 7.3.

bastará la simple solicitud[21], y cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

La propuesta de Reglamento comunitario mantiene una configuración del derecho de oposición similar a la de la Directiva del 95, previendo que ha de admitirse por razones propias de la situación del interesado al menos en los casos en que el tratamiento sea necesario para atender intereses vitales del interesado, sean recabados para el ejercicio de una misión efectuada en interés general o relevante para el ejercicio de la autoridad pública de que esté investido el responsable o en atención a intereses legítimos perseguidos por el responsable del tratamiento. También se recoge el derecho a oponerse al tratamiento de datos con fines de publicidad[22].

En cuanto a la cancelación, es el derecho que la Ley reconoce al afectado para retirar datos, en principio mediante su bloqueo, cuando el tratamiento no se ajuste a lo dispuesto en la Ley[23]. Una posibilidad es la recogida en el apartado 5 del artículo 4 de la LOPD cuando establece que los datos personales serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados y no serán conservados en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubiesen sido recabados o registrados.

Las tres facultades pueden ejercitarse frente al responsable del fichero o tratamiento y en el caso de los datos que son objeto del mismo en Internet será responsable quien decide o permite tanto la «subida» de los datos como su difusión en la red, pues en todos estos casos se están determinando efectivamente los fines y medios del tratamiento.

Se trata de tres facultades o derechos distintos aunque ni en la práctica ni en el propio tratamiento legislativo se aprecien claramente las diferencias. Sus condiciones de ejercicio son distintas. Mientras que la revocación y la oposición no presuponen irregularidad alguna en el tratamiento de los datos la cancelación está prevista, precisamente, para esta última eventualidad, aunque si el interesado revoca el consentimiento y el responsable lo mantiene se producirá una vulneración de la LOPD que posibilita la cancelación. En definitiva, el ejercicio de los derechos de oposición y cancelación ha de estar justificado de tal manera que no existe un derecho libre y absoluto a exigir la eliminación de los datos personales recogidos en cualquier fichero. Si se ejercita el derecho de oposición tienen que existir motivos fundados en una situación personal, salvo en relación con los datos obtenidos con fines publicitarios o de prospección comercial. El presupuesto de la cancelación es, precisamente, el incumplimiento de la norma por parte del responsable del tratamiento. Por último, en el caso de revocación, si el ejercicio de la misma genera perjuicios que la otra parte no tenga obligación de soportar, como por ejemplo cuando se produce en el marco de una relación contractual, hemos defendido que la revocación puede conllevar una indemnización.

21 Cfr. art. 51 RD 1720/2007.

22 Cfr. art. 19.

23 Art. 16.

Precisamente uno de los fines de la propuesta de Reglamento comunitario es recoger lo que se ha dado en llamar derecho al olvido digital, cuyo significado a día de hoy es equívoco. Al no ser «todavía» un concepto legal no se sabe si cuando se alude a ello se quiere hacer referencia a un derecho de eliminar los datos personales con motivo o justificación cuando se requiera, de manera que en realidad se trataría de ejercitar las facultades de revocación, oposición o cancelación, o al derecho absoluto al que antes me he referido. En muchos casos a lo que realmente se alude es a un pretendido derecho a la desindexación de los datos en la red de tal manera que los buscadores y motores de búsqueda, salvo consentimiento, no permitan acceder a los mismos aun cuando aparezcan en la página web original, ya que realmente lo que propicia la difusión no querida es la indexación.

En relación con esta cuestión el artículo 17 de la Propuesta de Reglamento establece que el interesado tiene derecho de obtener del responsable del tratamiento la eliminación de los datos que le conciernan, así como su difusión, en especial cuando se trate de datos proporcionados por el interesado siendo menor, por alguno de los motivos que relaciona: que los datos no sean ya necesarios para los fines para los que han sido recogidos o tratados, que el consentimiento haya sido retirado o haya expirado el tiempo autorizado para la conservación y no exista otro motivo legal para la misma, la oposición al tratamiento o que el tratamiento no sea conforme al Reglamento por otros motivos. En definitiva, no parece que el «nuevo» derecho al olvido y a la eliminación de los datos se configure como facultad distinta de la revocación del consentimiento, la oposición y la cancelación, de tal manera que puede concluirse que no es más que la manera de hacer referencia generalizada al ejercicio de aquellas facultades, con el contenido que cada una de ellas tenga. La consecuencia del ejercicio legítimo del derecho es, lógicamente, que el responsable ha de proceder inmediatamente a la eliminación de los datos, pero se prevén excepciones que nuevamente lo modalizan, pues puede autorizarse la conservación posterior por fines de investigación histórica, estadística y científica, por razones de interés público en el ámbito de la salud pública, para el ejercicio del derecho a la libertad de expresión, cuando la legislación lo exija, o en caso de que existan motivos para restringir el tratamiento de los datos en vez de proceder a su supresión (cfr. Considerando 53).

5. PROBLEMAS CONCRETOS

5.1. Ejercicio de los derechos de oposición y/o cancelación frente a un buscador

La mayor parte de las reclamaciones presentadas ante la Agencia Española de Protección de Datos con esta finalidad y que, siendo acogidas por la misma, fueron seguidamente recurridas ante la Audiencia Nacional, iban dirigidas frente al buscador Google[24], solo o en compañía de otros, como responsable del tratamiento por el cual los datos personales de un sitio web resultan indexados y se hacen accesibles para cualquiera que realice determinadas

24 La mayoría contra la filial española Google Spain S.L. y alguna contra Google Inc.

búsquedas. Al margen de la alegación de Google de que no se encuentra sometido al Derecho de la Unión Europea ni al español por tener la empresa la sede en Estados Unidos y que vamos a obviar en este trabajo, el buscador se defiende, respecto de la cuestión de fondo, argumentando que quien sería en su caso responsable es el titular del sitio web en el que los datos se hacen públicos originariamente. Se plantea, por tanto, cuándo y en qué medida existe, si es que existe, un derecho a oponerse al tratamiento de los datos o a cancelarlos frente a cada uno de los implicados, la webmaster que edita originariamente los datos, por una parte y el buscador que mediante la indexación de los mismos favorece su difusión, por otra.

Si bien para considerar a los buscadores responsables del tratamiento la Agencia tiene en cuenta su carácter de prestadores de servicios de la sociedad de la información según la Ley 34/2002 de 11 de julio, entiendo que se trata de ámbitos distintos[25]. Como ya se ha dicho, los buscadores serán responsables del tratamiento de datos personales en la medida en que efectivamente determinen los fines y medios del mismo, al margen de su carácter de prestadores de servicios de la sociedad de la información y de las obligaciones y responsabilidades que puedan tener en este ámbito. Precisamente la primera de las preguntas que presenta la Audiencia Nacional, en el Auto de la Sala de lo Contencioso-Administrativo de 27 de febrero de 2012, es si debe interpretarse que la actividad de Google consistente en localizar la información publicada o incluida en la red por terceros, indexarla automáticamente, almacenarla temporalmente y ponerla a disposición de los internautas, está comprendida en el concepto de «tratamiento de datos» que ofrece la Directiva 95/46/CE.

En mi opinión si, como hemos visto más arriba, el ámbito de aplicación de la normativa de protección de datos viene determinado por el hecho de que los mismos se encuentren en un soporte físico con una cierta organización o estructura a partir del cual el responsable del tratamiento dispone de los mismos, en la actuación de cualquier buscador se dan todos los presupuestos, aunque no sean directamente proveedores de contenidos. Mediante las llamadas «arañas» rastrean los datos presentes en la red organizándolos de forma que cualquier persona pueda acceder a ellos si realiza determinadas búsquedas.

En caso de que la publicación de los datos en el sitio web originario sea ilegítima parece evidente que el primer responsable será el editor de los datos pero ello no obsta para que el titular de los mismos pueda también ejercer frente al buscador su derecho de cancelación,

25 Aunque la Audiencia dice que se pregunta si las empresas titulares de los buscadores son responsables «cuando actúan como proveedores de contenidos», precisamente se le plantea la duda por el automatismo con que se produce la captación de la información y por la ausencia de un control efectivo sobre la misma, especialmente sobre la exactitud y veracidad de la información que los buscadores indexan. En realidad los buscadores no son proveedores de contenidos sino prestadores de servicios de intermediación. También es cierto que actualmente se puede observar un doble ámbito de actuación de estos operadores, la mera intermediación tradicional, por una parte, y una actividad más compleja de almacenamiento de los datos obtenidos por distintos medios, cruzándolos después para obtener perfiles de los usuarios, por otra, lo que parece que va más allá de una mera actuación instrumental (Vid. Dictamen del Grupo del artículo 29 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda, 00737/ES WP 148). Pero lo cierto es que la actividad a la que se refiere la Audiencia no es esta última sino la mera intermediación.

pues la normativa no se lo impide. No habiendo previsión en otro sentido el titular de un derecho fundamental que claramente ha sido lesionado ha de poder actuar frente a todos aquellos que causen o coadyuven en la lesión, máxime cuando puede incluso darse el caso de que el titular de la página web original ya no exista o sea ilocalizable. La Ley de Servicios de la Sociedad de la Información avala esta solución al establecer en su artículo 8 que en caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra determinados principios entre los que se encuentra la dignidad de la persona, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran y en el 17 que, con independencia de que por supuesto los buscadores, como intermediadores que son, no tienen una obligación de control «a priori» de los contenidos indexados, serán responsables y, por tanto, habrán de soportar las consecuencias que de ello se derive, en caso de que tengan conocimiento efectivo de que la actividad a que remiten o recomiendan es ilícita – en este caso tratamiento ilícito de los datos- y no adopten las medidas necesarias para impedir el acceso a las mismas[26]. En definitiva, el hecho de que la web en la que originariamente se publiquen los datos haya dejado la puerta abierta al no impedir su indexación no justifica una entrada que lesione un derecho fundamental en aras del modelo de negocio de un buscador.

Pero ocurre que en los casos que han llegado a la Agencia y que han sido recurridos ante la Audiencia Nacional el tratamiento de los datos en la web original, al menos inicialmente, es legítimo, de tal manera que el derecho a ejercitar para poder eliminar los mismos es el de oposición, que prosperará cuando exista un motivo también legítimo y fundado[27] y la Agencia, apoyándose en los citados artículos 8 y 17 de la Ley de Servicios de la Sociedad de la Información, está exigiendo igualmente al buscador la adopción de las medidas necesarias para retirar los datos de su índice e imposibilitar el acceso a los mismos[28]. Entiendo que hay casos en los que también podría justificarse. Es posible que pese a la licitud inicial del tratamiento de los datos la continuidad de su publicidad lo haga devenir ilegítimo en cuyo caso podría mantenerse la postura anterior. Pero también puede ocurrir que sea precisamente la accesibilidad facilitada por los enlaces que proporcionan los buscadores, aunque sea neutralmente, la que hace que el tratamiento de los datos, lícito en su origen se convierta en desproporcionado y, por tanto, contrario a la normativa de protección de los mismos. Con independencia de que teniendo en cuenta la necesaria adecuación de los datos a los fines del tratamiento pueda imponerse a los responsables de las webs originales – por ejemplo de un

26 Otra cuestión que excede de los límites de este trabajo son los problemas que puede plantear la interpretación que está haciendo el Tribunal Supremo del requisito del «conocimiento efectivo» de la ilicitud.

27 Así, en la Resolución R/01746/2011, la AEPD considera que no procede la oposición al tratarse de datos relativos a un proceso selectivo de una Administración Local, que se había realizado hacía muy poco tiempo, sin acreditar que fueran inexactos o que hubiesen quedado obsoletos.

28 Vid., por todas, la Resolución R/01199/2010, consecuencia de una solicitud de cancelación de los datos que aparecen en el sitio web en el que se publica el Boletín oficial de una provincia.

boletín oficial - la obligación de evitar la indexación, y de hecho la Agencia Española de Protección de datos lo ha «recomendado» en varias de sus resoluciones[29] desde la perspectiva del titular del derecho fundamental afectado es defendible que pueda dirigirse también frente al buscador o buscadores que posibilitan la difusión de los datos con el fin de que adopte las medidas necesarias para evitar el acceso.

No obstante, a la Audiencia Nacional se le plantean dudas respecto de la posibilidad de requerir a Google para que retire de su buscador la información contenida en la página web de un tercero porque aquel no puede discutir la licitud o exactitud de una información que ni ha publicado ni puede modificar sino que es el titular de la página web el que controla la información y el que puede defender el mantenimiento de la misma frente al afectado. Además se considera que la supresión o cancelación de los datos del buscador podría incidir en los derechos del titular de la página web (tales como el derecho de información, liberad de expresión y otros) o el cumplimiento de las obligaciones legales que tiene contraídas sin que haya tenido oportunidad de defenderlos.

Creo que por una parte esos peligros no son tan evidentes y, por otra, se me plantea la duda, que parece compartir la Audiencia, de si aunque efectivamente existan ello justificaría la limitación en la protección del derecho fundamental a la protección de datos pues, de acuerdo con las circunstancias de cada caso concreto, es posible que haya de prevalecer sobre otros derechos e intereses en juego. En primer lugar el buscador, ante el requerimiento del afectado, que deberá de hacer referencia concreta a los datos a los que se refiera y fundamentar su petición, estará en condiciones de defender la licitud de su propia actividad de indexación. Por otra parte, no creo que la posibilidad de que la supresión o cancelación de los datos del buscador pueda incidir en derechos del titular de la página web como la libertad de expresión o información, ya que se ejercen mediante la publicación de las informaciones u opiniones en el sitio web y no mediante la posibilidad de indexar las mismas. El buscador, en su caso, no impediría la información, sino su difusión indiscriminada, desproporcionada u obsoleta. Por último, tampoco se entiende bien la posición tan radical de Google cuando en su propia política de privacidad propicia que los usuarios puedan evitar que aparezca información personal en el buscador de lo que se deduce que ni lo considera inadecuado ni técnicamente inviable[30].

Con esto no se quiere decir que no se planteen problemas importantes y que tanto los ya mencionados como otros presentados por la Audiencia Nacional hacen difícil llegar a una solución indiscutible. Además, es importante la necesidad de ponderar la proporcionalidad de una medida de esta naturaleza frente al fundamento del ejercicio de las facultades de oposición y cancelación. Cuestiones como la dificultad técnica para cumplir la finalidad que se persigue sin dañar los derechos de terceros – por ejemplo, eliminar de los índices un de-

29 En este sentido serán los responsables principales, que quizá sea a lo que quiera referirse el Grupo de Protección de Datos del artículo 29 cuando califica a los buscadores de responsables subsidiarios.

30 Cfr.http://support.google.com/setmasters/bin/answer.py?hl=es&answer=164133&topic=1724262&ctx=topic

terminado nombre y apellido impediría también el acceso a la información referente a todas las personas que tengan el mismo - y la ineficiencia que para la protección de datos supone el hecho de que no se elimine del sitio web inicial y la reclamación se dirija solamente frente a un buscador, hace que esperemos con expectación la contestación del Tribunal de Justicia.

Por último, la Audiencia pregunta sobre el contenido actual del llamado derecho al olvido al que antes nos hemos referido y, en definitiva, sobre si los derechos de supresión, bloqueo de datos y oposición incluyen la posibilidad de que el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros y manteniendo, por otra parte, la información que le beneficie. Se entiende que una actividad de esta naturaleza pueda ser tachada de fraudulenta desde muchos sectores pero también hay que tener en cuenta que, sin perjuicio de su ponderación con otros derechos e intereses en juego, el poder de disponibilidad de los propios datos, sobre todo si se trata de informaciones que incidan directamente en la intimidad, deriva de la propia dignidad del ser humano.

5.2. Ejercicio de las facultades de revocación, oposición y/o cancelación frente a otros eventuales responsables del tratamiento

Algunas de las reclamaciones que han llegado a la Agencia se deben a datos personales publicados en páginas web de medios de comunicación. Como ya se ha dicho, las noticias o comentarios publicadas en prensa u otro medio, incluso a través de un sitio web, están protegidas en principio por las libertades de expresión y/o información cuya trascendencia para la formación de una opinión pública libre les proporciona una posición prevalente respecto de otros derechos constitucionales con los que pueden entrar en colisión como el derecho al honor, a la intimidad o a la protección de datos personales como aspecto de la privacidad. En los conflictos que se han mantenido ante los Tribunales españoles la ponderación de los derechos de protección de datos y libertad de expresión e información ha llevado a soluciones diferentes según los casos y las circunstancias. Hay que tener en cuenta, en todo caso, la tendencia jurisprudencial de reservar las libertades informativas para los medios de comunicación, lo que ha llevado, en materia de protección de datos, a sanciones por la publicación de los mismos en una página web cuyo titular no era un medio de comunicación[31] y a la confirmación de las mismas por los Tribunales[32]. También es cierto que en otros casos

31 Dice la AEPD en la Resolución 211/2010 que «las páginas web del imputado no pueden ser consideradas medios de comunicación social sin que quepa invocar el ejercicio y prevalencia del derecho de libertad de información que derivaría en una prevalencia general que aboliría e ipso la protección de datos personales».

32 En la STS de 26 de junio de 2008 el alto tribunal considera procedente la sanción impuesta por la APD contra la Asociación contra la tortura que, en una página web, difundía información sobre Guardias Civiles condenados, considerando que tales contenidos estaban excluidos de la libre expre-

la AEPD ha manifestado que las afirmaciones en un foro o en general en la web son ejercicio de la libertad de expresión[33]. Por su parte, la Propuesta de Reglamento de la Unión Europea entiende necesario interpretar en sentido amplio conceptos relativos a la libertad de expresión de manera que en el caso de que sea aprobado los Estados miembros deberán clasificar determinadas actividades como «periodísticas» a los efectos de las exenciones que puedan adoptarse al amparo del Reglamento si el objeto de las actividades es la comunicación al público de informaciones, opiniones o ideas, con independencia del medio que se emplee para difundirlas y que no tiene por que circunscribirse a empresas de comunicación, pudiendo desarrollarse con o sin ánimo de lucro[34].

Para poder analizar otro supuesto conflictivo, la publicación de sentencias judiciales en la red, hay que partir de la situación jurídica actual de la publicidad de las actuaciones judiciales, regulada por los artículos 223 y 266 de la Ley Orgánica del Poder Judicial y por el Acuerdo de 15 de septiembre de 2005 del Pleno del Consejo por el que se aprueba el Reglamento 1/2005 de los aspectos accesorios de las actuaciones judiciales[35]. Por lo que se refiere a la publicación oficial de las sentencias, a la que se refiere el artículo 107.10 de la LOPJ, el citado acuerdo exige que en el tratamiento y difusión de las resoluciones judiciales se cumpla lo dispuesto en la legislación en materia de protección de datos personales y que, a salvo lo establecido en la LOPJ, los órganos judiciales no faciliten copias de las resoluciones. En este sentido la sentencia de la Audiencia Nacional de 13 de junio de 2007 considera que no pueden difundirse las sentencias con datos de carácter personal que permitan la identificación de las personas en cuestión a no ser que cuente con su consentimiento o que concurra alguna de las causas contempladas en el artículo 6.2 de la LOPD, fundamentalmente cuando se haga en ejercicio de la libertad de información, lo que como hemos dicho ocurrirá sobre todo cuando sea precisamente un medio de comunicación el que la haga pública.

También la difusión de los datos que los buscadores indexan desde las páginas de los diferentes boletines oficiales que existen en nuestro país está dando lugar a muchas reclamaciones. Aunque el tratamiento de los datos por los diarios oficiales está amparado por la leyes es posible que el transcurso del tiempo haga que el tratamiento devenga ilícito como ocurrirá, por ejemplo, cuando los datos sigan siendo públicos indiscriminadamente en la red tras su conservación durante un tiempo desproporcionado para el fin para el que se acordó la publicidad –por ejemplo, notificación de actos administrativos respecto de los cuales el interesado ya se ha dado por notificado – o que la difusión pueda tacharse de excesiva por tratarse de diarios oficiales de ámbito territorial limitado. En estos casos la Agencia, con

sión e información, afirmando que «la libertad de información alcanza su máximo nivel cuando la libertad es ejercitada por los profesionales de la información a través del vehículo institucionalizado de formación de opinión pública».

33 Sobre estas cuestiones puede verse Cotino Hueso, I. (2010) Datos personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público en *Comentario a la Ley orgánica de protección de datos de carácter personal*, Troncoso Reigada, A. (dir.), cit., pp. 295 ss.

34 Vid. Considerando 121.

35 También es especialmente relevante la STC de 3 de marzo de 1995.

independencia del requerimiento al buscador, considera que también los responsables del boletín deben limitar la indexación de los datos personales de los interesados[36].

En definitiva, parece claro que en muchos casos lo que realmente provoca el problema es la difusión indiscriminada a la que aboca la indexación por los buscadores. En consecuencia, además de la posibilidad ya analizada de obligarlos a eliminar los datos de sus índices o a impedir el acceso a ellos, se plantea si se puede imponer a los titulares de la página web que los hace públicos, en principio lícitamente, la carga de adoptar las medidas técnicas necesarias para impedir dicha indexación, bien desde un principio o bien como consecuencia del ejercicio de las facultades de revocación, oposición o cancelación.

La respuesta es difícil y sin duda ha de tenerse en cuenta cada caso concreto. Ciertamente determinados instrumentos como los periódicos o los boletines oficiales tienen precisamente una finalidad de publicidad. Hay que partir, por tanto, de que el hecho de que se consiga más publicidad gracias a «subir» el documento a la red, en principio es positivo pues ofrece un *plus* de aquello que precisamente se pretendía. No obstante, puede defenderse la obligación de tomar medidas para hacer anónimo o evitar la indexación y difusión de los datos una vez transcurrido un periodo de tiempo (el plazo dependerá de del caso concreto y de que venga o no establecido en una disposición legal) teniendo en cuenta aquella obligación de cancelación de los datos cuando ya no sean necesarios de acuerdo con el artículo 4 de la LOPD. Incluso cuando la publicidad de los datos es lícita, la Agencia sugiere igualmente que los medios de comunicación valoren la necesidad de que su actuación se dirija a conciliar, en mayor medida, el derecho a la libertad de información con la aplicación de los principios de protección de datos personales. En este sentido insta a ponderar escrupulosamente la relevancia pública de la identidad de las personas afectadas para, en el caso de que no aporte información adicional, evitar la identificación mediante la supresión del nombre e incluso, si fuera necesario de las iniciales o cualquier referencia suplementaria de la que pueda deducirse la identificación en el caso de que el entorno sea limitado.

En cuanto a las redes sociales, la cuestión de la protección de los datos personales es especialmente importante tanto porque muchos usuarios no son conscientes ni de que los datos personales de otras personas, incluidas fotografías, no pueden hacerse públicos sin su consentimiento, ni del riesgo real de difusión de los propios datos.

Problemas de aplicación territorial aparte, según la legislación comunitaria y, más en concreto la española, los titulares de redes sociales son prestadores de servicios de la sociedad de la información que, en la medida que tiene como actividad principal el almacenamiento de información que contiene múltiples datos personales y ponerla a disposición de los otros miembros del sitio, es responsable del tratamiento de los datos. Téngase en cuenta que, aun cuando el usuario no tenga necesariamente que identificarse públicamente de acuerdo con las condiciones del acuerdo que le une con la red, la propia finalidad de la misma le llevará a hacerlo y, aun cuando pudiera darse el caso de no identificarse, sería identificable precisamente por la información que suministra y por el propio comportamiento en la red.

36 Informe de la Agencia Española de Protección de datos 0214/2010.

Aunque los usuarios presten su consentimiento aceptando las condiciones que les impone el titular de la red y subiendo sus datos a la misma, este puede no ser válido si no se han cumplido todos los requisitos de información del artículo 5 de la LOPD, incluyendo en la misma si se recogen cookies e informando sobre todas las finalidades del tratamiento con fines distintos a la participación en la red social, como puede ser el marketing o la publicidad[37]. La problemática alcanza también a una eventual revocación del consentimiento pues aunque la obligación del responsable del tratamiento de acceder a la solicitud no parece que pueda resultar discutida ni aun cuando pudiera considerarse que el acuerdo que une al afectado con el titular de la red social tenga naturaleza contractual, técnicamente la eliminación definitiva de los datos puede resultar imposible.

6. CONCLUSIÓN

Nos encontramos ante una materia cuyo régimen jurídico está en proceso de cambio y pueden adoptarse pocas conclusiones definitivas. De ellas quizá la más relevante sea que la necesidad de encontrar el equilibrio entre intereses contrapuestos, que es tarea general del derecho, se concreta aquí en que el deseable desarrollo de las nuevas tecnológicas y de la sociedad de la información no puede producirse de espaldas a los derechos básicos de las personas, pero que estas han de ser también consecuentes y saber que el uso de aquellas y los beneficios de todo orden que proporcionan conlleva inevitables riesgos e incluso renuncias que, en ocasiones, hay que asumir.

7. BIBLIOGRAFÍA

Arias Máiz, V. (2010). Una excepción al principio del consentimiento informado no contemplada en el artículo 6 LOPD: el uso de datos personales por medios de comunicación en *Comentario a la Ley Orgánica de protección de datos de carácter personal*, Troncoso Reigada (dir.), pp. 560 – 577.

Cerrillo-i-Martínez, A., Peguera, M., Peña-López, I. & Vilasau Solana, M. (coords.) (2011). Neutralidad de la red y otros retos para el futuro de Internet. Actas del VII Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona 11-12 de julio de 2011. Barcelona: UOC-Huygens.

37 Además, habrá de informarse acerca de todas las posibilidades de acceso, de qué datos van a ser cedidos y si se va a hacer publicidad, si la información va a ser indexada por motores de búsqueda, etc. (Vela Sánchez Merlo, C. (2010). Tratamientos privados de datos del artículo 25 de la LOPD: el ejemplo de las redes sociales en Comentario a la Ley orgánica de protección de datos de carácter personal, cit., pp.1485-1513).

Cotino Hueso, I. (2010). Datos personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público en *Comentario a la Ley orgánica de protección de datos de carácter personal*, Troncoso Reigada, A. (dir.), pp.295-323.

Fatás J.M., García Sánz, M. (2008) en *Comentario al Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal*, Aranzadi: Navarra.

Lolin, C. y Poullet, U. (2011). Sociedad de la información y marketing: case study (traducción de María Rosa Llácer Matacás) en *Protección de datos personales en la sociedad de la información y la vigilancia*, Llácer Matacás, M.R., (coord.), Madrid: La Ley, pp. 231-277.

Marín López, J. (2012). El tratamiento de datos personales sin consentimiento del interesado tras la sentencia del Tribunal Supremo, Sala 3ª, de 8 de febrero de 2012, http://www.diariolaley.es, diario de 24 de febrero de 2012.

Martínez Martínez, R., (2011). «Interés legítimo y protección de datos en la sentencia de 8 de febrero de 2012», http://www.elderecho/com/administrativo/Interes-proteccion-personales-Tribunal-Supremo_11_372805001.htlm.

Moiny, J-P., (2012). «Facebook y la Directiva 95/46. Algunas reflexiones» (traducción de María Rosa Llácer Matacás) en *Protección de datos personales en la sociedad de la información y la vigilancia*, Yacer Matacás, M.R., (coord..), Madrid: La Ley, pp. 277-320.

Orza Linares, R. y Ruiz Tarrías, S. (2011). El régimen constitucional del derecho al olvido en Internet en *Neutralidad de la red y otros retos para el futuro de Internet. Actas del VII Congreso Internacional Internet, Derecho y Política*. Universitat Oberta de Catalunya, Barcelona 11-12 de julio de 2011 (Cerrillo-i-Martínez, A., Peguera, M., Peña-López, I. & Vilasau Solana, M., coords.). Barcelona: UOC-Huygens.

Vela Sánchez Merlo, C. (2010). Tratamientos privados de datos del artículo 25 de la LOPD: el ejemplo de las redes sociales en *Comentario a la Ley orgánica de protección de datos de carácter personal*, Troncoso Reigada (dir.), pp. 1485-1513.

REVIVING PRIVACY: THE OPPORTUNITY OF CYBERSECURITY

Maria Grazia Porcedda
Department of Law,
European University Institute, Research assistant

ABSTRACT: The online entertainment industry has thrived thanks to unprecedented technical innovations and responsive organizational changes, whose combination is challenging privacy and data protection in two respects. Firstly, they are affected by those business models based on the provision of *seemingly* free services, in the subtle exchange for as much personal information as possible.

Secondly, the multiplication of online devices, users and services, cloud computing and big data raise issues of technical security, i.e. cybercrimes and cyber-security, and affect privacy and data protection when personal information is affected.

Moreover, due to the relevance of Critical Information Infrastructure to the national economy and security, governments are starting to tackle cyber-challenges. Yet, the policy debate is focussing excessively on traditional crimes committed by electronic means, which are quite different from novel crimes possible only in the online environment, and on surveillance measures. This may bias the choice of the best means to tackle cyber-crimes and further challenge privacy and data protection, mostly seen as an obstacle to investigations.

However, I maintain that, in theory, the adoption of cyber-security policies represent more an opportunity to revive privacy and data protection than a threat. Not only is privacy built into classic computer security paradigms, but the data protection regime also contains provisions whose implementation in a cyber-security policy may act as a proxy to reduce cyber threats, provided that a number of conditions are respected. Part of the problem, and therefore the solution, may lie in appropriately redistributing responsibility and accountability online.

KEYWORDS: privacy, data protection, cybercrime, cyber-security, economics of privacy, information society services.

1. INTRODUCTION

This paper addresses the dire challenges to privacy and data protection arising from the combination of technical innovations and related organizational changes that led, among others, to the success of the online entertainment industry.

Firstly, the business model[1] of some of the most thriving online (entertainment) businesses rests on the provision of *seemingly* free services, in the subtle exchange for as much

1 (Anderson C., 2009).

private data as possible; thus, assertions concerning the 'death' or 'irrelevance' of privacy abound.[2]

Secondly, the increasing number of online devices and users, the multiplication of services, cloud computing and big data raise issues of technical security, i.e. cybercrimes and cybersecurity, thus undermining privacy and data protection when personal information is affected, but not only. Due to the relevance of Critical Information Infrastructure (hereafter CII)[3] to the national economy and security, governments are starting to tackle cyber-challenges. Yet, different interpretations of what constitutes a 'threat' are pushing governments to give the military room of manoeuvre to police the internet, or to surveille communications to curb opposition.

Furthermore, the policy debate is focussing excessively on traditional crimes committed by electronic means (broad cyber-crimes), which are profoundly different in terms of underlying logics from novel crimes possible only in the online environment (narrow cybercrimes). This may actually bias the choice of the best means to tackle cyber-crimes, unduly challenge the liberties involved – like privacy and data protection, mostly seen as an obstacle to investigations – and close a precious window of opportunity to revive privacy.

In fact, while privacy and data protection may be affected by the adoption of policies tackling cyber-crime and cyber-security in the European Union (hereafter EU) and elsewhere, this paper maintains that the adoption of cyber-security policies represents more an opportunity to revive privacy and data protection than a threat. Not only is privacy built into classic computer security paradigms, but the data protection regime also contains provisions (i.e. those on security), whose implementation in a cyber-security policy may act as a proxy to reduce cyber threats, and in particular narrow cybercrime, provided that a number of conditions are respected.

This discussion is particularly timely, due to the revision of the Data Protection regime and[4] the Council Framework Decision on Attacks against Information Systems[5] in the EU, on which this paper focuses, as well as the growing international cooperation, which is leading to common activities such as in the case of the EU-US Working Group on Cybersecurity and Cybercrime (hereafter WGCC).[6]

---

2 Similar claims have been repeatedly made since the invention of the mainframes. See in (Rodotà, 1973).

3 CIIs are «ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).» In turn, Critical Infrastructure (CI) are «those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments.» (European Commission, COM(2005) 576 final), pp. 19-20.

4 (European Commission, General Data Protection Regulation, COM(2012) 11 final); (European Commission, COM(2012) 10 final).

5 (Council Framework Decisions 2005/222/JHA, OJ L 69, 16.3.2005, p. 67); (European Commission, COM (2010) 517 final); (Council of the European Union, 11566/11, 2011).

6 (Porcedda M. G., Transatlantic Approaches to Cyber-security and Cybercrime, 2011).

In the following sections I will first analyse how the specific drivers for the success of the online (entertainment) industry are affecting privacy and data protection, and then specifically focus on cybercrime and cyber-security. I will then explain how privacy and data protection can be complementary to the pursuit of cyber-security, and, in the conclusion, explain how the online entertainment industry matters and has responsibility for the subject.

2. ORGANIZATIONAL AND TECHNICAL CHALLENGES TO PRIVACY AND DATA PROTECTION

The growth and flourishing of the internet, and the online (entertainment) industry is the result of important technological developments, which occurred in the last decade, as well as responsive organizational practices.

First of all, the internet network infrastructure has grown tremendously, thanks to a combination of cable, satellite, radio waves, infrared, laser signals and fibre optic networks. Also, the success of Moore's first law[7] results in increasingly cheaper personal computers, 3G and 4G-based smartphones and videogames consoles[8] allowing internet access. Consequently, more people than ever can be reached by, and enjoy, services online.

Secondly, the Web 1.0 has evolved into the Web 2.0 and user generated content (UGC), whereby users have become active creators of content in the form of text, voice and images, which is indexed and thus made available on the internet. This triggered the development of social networking sites (Facebook, Google+, Linkedin), UGC platforms (blog hosts) and audio-visual content on demand (i.e. YouTube, MySpace, Netflix).

Thirdly, cloud computing (SaaS, Paas and Iaas), which marks the return of shared computing, provides unprecedented storage capacity and processing resources availability for both SMEs and individuals. Also, by detaching storage from one's machine, the cloud allows one to access the data from anywhere, and, due to the distribution of data centres, brings about data dispersion (aka 'feeling of location independence'), leading to constant data flows.[9] As such, the cloud provides the infrastructural backbone for the development of the entertainment industry. In addition, an emergent effect of the cloud is that deleting information has become more costly than storing it, thus fuelling the so-called era of 'big data',[10] which paves the way to new business opportunities.[11]

Finally, data processing techniques have improved, thus leading to more refined collection, storage, aggregation, analysis, linking and creation of inferences of (big) data, which in

7 Whereby processors speed doubles every year and a half (18 months).

8 (OECD, 2011).

9 (Kushida et al., 2011).

10 (Thiele, 2012). See also (Lohr, 2012).

11 (World Economic Forum, 2012); (Darrow, 2012).

turn is showing the limits of current anonymisation techniques. This allows companies to better 'extract value' from data, in order to offer new services and applications.[12]

Obviously, these technological developments would have not been sufficient to foster a successful entertainment industry without appropriate organizational practices.[13] Yet, this very same combination of technological improvements and business model(s) are threatening privacy and data protection in two distinct ways.

2.1. Challenge n. 1: Surreptitious barters

Some of the most successful companies in the entertainment industry are thriving thanks to a business model allowing to 'generate revenue' by means of customized advertisement[14] 'linked to free services'.[15] It may be more correct to say 'ostensibly free services', because users are actually paying with their personal data (reportedly, each user's profile was worth $4 to Facebook and $24 to Google last year)[16] and cannot really choose whether to give information or not, due to 'take it or leave it' terms of use, provided they are aware of such surreptitious barter.

In fact, the terms of use and privacy policies are often written in a legalistic, obscure language, and prevent users from understanding how their personal information will be used and what strategies to adopt in order to protect themselves.[17] In other words, the terms of use do not explain that the information given about oneself (or about others) will be stored and sold to third parties (or unduly accessed and used[18]), to perform analytics, mostly for targeted advertising, but for other purposes, too. Nor is there clear information relating to the persistence, memory and searchability of the products of online (as opposed to offline) sociality, which becomes crucial as users increasingly publish information about third, unaware, parties.[19]

Ironically, while the increase of personal data flows translates into a wider scope of application of privacy rules,[20] thus raising their importance, users' privacy is endangered at unprecedented levels.[21] From a legal perspective, businesses applying 'surreptitious barters' thrive thanks to a constant bypassing, if not violation, of privacy and data protection principles,[22] as understood in the EU, such as: consent, purpose limitation, data minimi-

12 (OECD, 2011); (Ohm, 2010).

13 (Loayza, 2009).

14 (Eckersley, 2009).

15 (OECD, 2011).

16 (Brushtein, 2012).

17 (OECD, 2011).

18 (Bilton, 2012).

19 (OECD, 2011). See also at http://www.garanteprivacy.it/garante/doc.jsp?ID=1585131.

20 (OECD, 2011).

21 (Andrews, 2012).

22 (Eckersley, 2009).

sation, the right of access and correction, and the norms on data transfers. Accordingly, to address similar failures and unforeseen technological developments,[23] data protection rules are being updated, as analysed later in this paper.

Meanwhile, lacking proper enforcement, personal data giants are emerging, such as Facebook, Google and Amazon, whose intentions and boundaries are unclear,[24] but whose centralized information can be a goldmine for potential wrongdoers.

2.2. Challenge n. 2: Cyber wrongdoings

In fact, and secondly, in accordance with the old saying whereby crime follows opportunity, the same technological and organizational innovations at the base of the development of an online (entertainment) industry have created new opportunities for crime, in the form of cybercrimes.

Online gambling sites, for instance, have been victims of cyber-extortions, which seem to work as follows: gambling sites' servers are attacked by means of a Denial of Service (hereafter DoS), or Distributed Denial of Service (hereafter DDoS) attack,[25] and owners are offered a solution to the problem in exchange for a ransom.[26] Another typical form of cybercrime for the entertainment industry is data breaches to acquire (financial) information. A recent illustration of the latter is the case of the double Sony PlayStation Network[27] and Sony Online Entertainment[28] security breach in 2011. Tens of millions of users were affected and their personal data stolen. The information included unencrypted credit card details,[29] which were reportedly sold in the black market. As a consequence, the company faced governmental investigations and collective actions, which could cost as much as US$ one billion,[30] without counting the damage to its reputation (a crucial criterion for allocating trust on the internet).

Several observations can be drawn from the Sony case. Firstly, it casts light on the potentially devastating effects of wrongdoings on the internet for the online (entertainment) industry.

---

23 Cloud computing and UGC platforms are, for instance, rendering the norms on controller and processor obsolete (Porcedda & Walden, 2011).

24 See (Hasbrouk, 2012).

25 «Denial of Service attack overwhelms Internet-connected systems and their networks by sending large quantities of network traffic to a specific machine. An attack from a single computer can easily be managed, and so attackers use large numbers of compromised machines to carry out Distributed Denial of Service (DDoS) attacks. Perpetrators must first take over the computers to be used for the attack, typically via email or web-based malware.» (Sommer & Brown, 2011), pp. 24-25.

26 (Sommer & Brown, 2011).

27 (Peckham, 2011).

28 (Arthur, 2011).

29 (Williams, 2011).

30 (Scarinci, 2012).

Secondly, it shows how cybercrimes like data breaches impinge upon users' privacy and data protection. Finally, it offers a good example of the complexity of what we call 'cybercrimes'.

In the terms of the Council of Europe Convention of Cybercrime,[31] for instance, the data breaches suffered by Sony entailed at least these two offences: illegal access to computer systems,[32] and computer fraud.[33] Actually, 'cybercrime' is a contested notion encompassing a number of different crimes targeting not only entertainment businesses, but also businesses at large, individuals, and the state, and calls for an analysis reaching far beyond the online entertainment industry.

2.2.1. What is really cybercrime?

Before analysing in greater detail how cybercrime and data protection interact, and in order to better explain it, I shall briefly illustrate the variety of offences encompassed by cybercrime. Many classifications are available, the only legally binding one (albeit widely criticized[34]) being that of the said Convention on Cybercrime, which informs the base of the EU legislation.[35] The Convention distinguishes crimes against the availability, integrity and confidentiality (i.e. the canonical goals of information security) of computer data and systems, from computer-related crimes, content-related crimes and copyright infringement.

The former category encompasses offences intimately linked to the cyber space, or narrow cybercrimes. These are:

- Illegal access (article 2), namely hacking and cracking, which leads to data security breaches (aimed or not at financial fraud) affecting businesses, individuals and states alike, e-espionage etc.;
- Illegal interception (article 3), namely the violation of confidentiality of non-public transmissions of data, which can lead to offences against the individual (i.e. identity theft, financial fraud) and against businesses and states (i.e. e-espionage, financial fraud);
- Data interference (article 4), namely malware, Trojans etc., which are at the base of botnets[36] (used to commit system interference, computer fraud and forgery), and attacks to the CII (i.e. the famous Stuxnet), which may lead to cyber-terrorism;[37]

31 Council of Europe, 'Convention on Cybercrime', 2001.

32 Article 2 of the Convention, which lays down rules on what is commonly referred to as hacking.

33 Article 8 of the Convention, which punishes the illegal transfer of property by means of a manipulation of data processing.

34 See (Porcedda, Transatlantic Approaches to Cyber-security and Cybercrime, 2011).

35 See (European Commission, COM(2005) 576 final).

36 Botnets are networks of computers (zombies) that have been infected by malware allowing remote control.

37 Cyber-terrorism can also be a controversial term, which needs «to be defined with the same precision as other forms of terrorist crime. There must be an intention and a real risk of causing death or serious bodily harm among members of the public, plus a terroristic intent, either to cause fear among the

- System interference (article 5), namely Dos, DDoS and spamming. DDoSs are often used for hacktivism against businesses (see the famous attacks by Anonymous to Visa and Mastercard) and states (attacks against the CII). Spamming often paves the way to phishing, leading to financial fraud against the individual; and
- Misuse of devices (article 6), namely the sale, procurement and distribution of hacking devices, which is at the base of many of the offences listed here.

The latter groups more traditional offences that can also be perpetrated in the cyberspace, or broad cybercrimes. These are further divided into:

- Computer-related crimes (articles 7 and 8): namely computer forgery (of electronic data with evidentiary value) and fraud (illegal transfer of property). I take the view that such offences can be considered narrow cybercrimes, since computer forgery and fraud are often committed by previously compromising computer systems (including smartphones[38]) by logical means (i.e. by using software such as malware, spy-ware, root-kits, zero day exploit attacks, logic bombs and Trojan horses);
- Content-related crimes, namely child pornography (article 9) and racist and xenophobic speech (introduced by an Additional Protocol), which are directed primarily against individuals; and
- Copyright infringement (article 10), which clearly affects businesses.

The list of offences is not exhaustive and wrongdoings such as identity theft, spoofing, synthetic identity fraud, website defacement, pharming, e-stalking, cyber-bullying etc., may not easily fall within the scope of the Conventions' provisions (whereas the so-called large-scale cyber-attacks are akin to some of the Convention's provisions, but are perpetrated on a wider scale). However, it should be manifest that the cybercrimes considered in this brief section are very different in nature, and the only common denominator is the online environment where they occur.

3. CYBERCRIME AND CYBERSECURITY: THREAT OR OPPORTUNITY?

Because of the importance of computer networks and systems as a component of CII for both government and private sector activities, their cross-sector interconnectedness, and the severe impact that offences occurring online can have, states have started addressing the issue of cyber offences. Therefore, governments in the EU and worldwide are adopting cyber security policies, i.e. policies relating to the security and stability of the CII, and cybercrime legislation, which include organizational and regulatory measures addressing the prevention, investigation and prosecution of cyber offences.

---

population or to compel the government to do or not to do something.» Martin Scheinin in (United Nations, 2009).

38 (Juniper Networks, 2012).

While this is timely and welcome, there are some reasons for concern, which stem from different interpretations of what constitutes a threat in cyberspace (and correspondingly the role of privacy), and from a 'do-what-is-feasible-and-visible-approach'. Such interpretations seem to be expressions of different communities in the cyberspace. It has been argued that two macro communities exist, one focusing on safety to people online and the other on the security of ICT systems,[39] roughly corresponding to broad and narrow cybercrime respectively, and which argue for different measures.

In addition, it has been asserted that within the community addressing the security of ICT systems, there would be a difference between «one, [which] focuses on individual systems and networks, has its roots in computer science and engineering communities; the other, a more recent concern, [which] focuses on collective and institutional systems, reflecting the influence of political and national security actors.»[40] These two communities hold two definitions of security, bearing different moral claims, and leading to different policy and technology outcomes, namely prevention or punishment (feasible since technology can accommodate any needs).

3.1. Notions of security (and privacy)

3.1.1. The broad cybercrimes community: security vs. privacy

What I call the broad cybercrimes community, which encompasses content-related offences (including cyber-bullying, e-stalking and e-blackmailing) and copyright infringement, seems to prefer a detection and prosecution-oriented approach in selecting priorities. This may have to do with a 'do-what-is-feasible-and-visible-approach'. Preventive practices, in fact, have to do more with persistent technologies, habits and behaviours than *ad hoc* technical solutions that swiftly fix the problem, and may be less visible. The result is a push towards increased surveillance. For instance, the anti-copyright infringement (which affects part of the entertainment industry) and anti-child pornography advocates lobby hard for the introduction of the habit of content filtering (that is, the curbing of net neutrality) by Internet Service Providers (hereafter ISPs).[41]

ISPs already carry out filtering for network security purposes, meaning to protect their own network from malware, which is both lawful and welcome. Here, the problem is that «in the online environment, what constitutes content is difficult to recognise: it's all code, whether it is a virus,[42] a political speech, or an image with child pornography.'[43] Therefore, filtering can be theoretically applied for any purposes, be it good or bad, from malware detection to surveillance (usually with the support of social techniques). In order to be

39 (Nash & Peltu, 2005).

40 (Nissenbaum, 2007), p. 59.

41 (House of Lords, 2007).

42 This means that filtering can be exercised for cyber-security purposes, which has been criticised by some as it may lead to the inhibition of the development of new protocols and applications.

43 (House of Lords, 2007). p. 23.

effective,[44] filtering should be applied at the end points of any communications, which means that users should be in charge of the final decision. This seems unrealistic; while expert users may accomplish the task well, beginners and unaware users are generally unable to recognise the risks and taking countermeasures. Unfortunately, the difference between expert and non-expert users is poorly addressed.[45]

This places ISPs in a better position to do so;[46] ISPs are actually using filtering techniques for traffic management purposes. The issue, however, is that there are several types of filtering,[47] each of them accomplishing different kinds of results, and having different impacts. «Certain inspection techniques involve the monitoring of content of communications, websites visited, emails sent and received, the time when it takes place, etc., enabling filtering of communications.»[48]

Content filtering of the type required by anti-child pornography and pro-copyright lobbies requires deep packet inspection, which is extremely intrusive from the point of view of privacy and data protection (and still requires human intervention[49]). In particular, it affects the confidentiality of communications, which is protected by article 8 of the European Convention on Human Rights[50] and the related jurisprudence, articles 7 and 8 of the EU Charter of Fundamental Rights,[51] as well as by article 5 of the e-privacy Directive.[52] This means that employing the most intrusive types of filtering requires a very strong oversight, to avoid unjustified purpose creep. The problem is that purpose creep is already taking place. A way to counter the practice would be to use end-to-end encryption, which is not welcomed by Law Enforcement Agencies (hereafter LEAs), because it could hide criminal activity.

Regrettably, the police lacks funds and cyber-training to focus on narrow cybercrime, which is affected by the problem of attribution, whereby it is difficult to identify logical attackers that only attack once (or that seem to be doing so). On the other hand, broad cybercrimes, which are the focus of many private-public partnerships,[53] give the impression

44 Moreover, filtering in general can be detected and bypassed, sometimes quite easily, and is exposed to false positives and negatives. The application of filters may lead offenders to use peer-to-peer instead, where content filtering is of no use, or the dark net. Ibid.

45 (Nash & Peltu, 2005).

46 ISPs, for instance, are active in the detection of botnets; an examples is the German anti-botnet initiative (see at http://www.oecd.org/dataoecd/42/50/45509383.pdf).

47 (Anderson & Murdoch, 2008).

48 (European Data Protection Supervisor, 2011).

49 See (Chen, 2012).

50 (Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 1950).

51 (European Union, 2000).

52 (European Data Protection Supervisor, 2011).

53 (Bahls, 2012). Public-private partnerships are not limited to broad cybercrimes. The EU-US WGCC, for instance, has launched private-public partnerships relating to botnets and supervisory

to be more easy to investigate and prosecute than narrow cybercrimes. Illicit content found thanks to filtering can be blocked or taken down, although this removes the symptoms without curing the disease: it has been shown that organized crime is responsible for child pornography (as well as other broad and narrow cybercrimes).[54]

In these circumstances, privacy and data protection become a value to be balanced against detecting the crime. This is because tackling broad cybercrime requires reactive measures, since the data are only an online 'projection' of a crime happening in the real world, and therefore constitute evidence, and not the object of the protection itself (which deeply differentiates the nature of broad and narrow cybercrimes).

3.1.2. Narrow cybercrime communities

a) The national security community: security vs. privacy

The national security community, which seems to be prevailing lately, focuses on collective existential harms which, in politics jargon, have been securitized. Some of the most recent policy statements, notably in the US, seem to suggest that an increased militarization of the cyber-space, fuelled by cyber-war(s) scaremongering,[55] is occurring, and call for the adoption of widespread surveillance measures. This is relevant due to the EU-US cooperation in the WGCC.[56] Cyber-security is increasingly referred to as a crucial national security issue, and the measures proposed either focus on deterrence or reaction, and preach increased surveillance, which reinforces the trends taking place to contrast broad cybercrimes.

Examples vary. For some governments, security concerns arise from the potential for the circulation of free information and the expression of dissent, and argue for additional surveillance.[57] Recently, China, Uzbekistan, Tajikistan and Russia have sent the UN president a joint letter calling for the adoption of an internationally agreed code of conduct for information security. An objective of such move would be to guarantee the respect of the policies adopted at the national level.[58]

For other governments, security concerns pertain to intrusion into and disruption of the CII, which is leading to the governmental and military attempt to assert general control over internet communications. In the United States, for instance, the Comprehensive Na-

control and data acquisition systems (SCADA). Further research is needed to address such a complex topic.

54 (Sommer & Brown, 2011).

55 (Brito & Watkins, 26 April 2011); (Lynn III, 2010); (Porcedda M. G., Transatlantic Approaches to Cyber-security and Cybercrime, 2011).

56 Ibid. (The White House).

57 (Rid, 2012).

58 (United Nations, General Assembly, 2011); Result of discussions held at the XXVII Isodarco Winter School, Andalo, January 2012.

tional Cyber Security Initiative (hereafter CNCI),[59] launched by President G.W. Bush and continued by President Obama, includes two programmes, Einstein 2.0 and Einstein 3.0, meant to protect governmental networks from attacks. Einstein 2.0 (CNCI n. 2) «is capable of alerting US-CERT [Computer Response Emergency Team] in real time to the presence of malicious or potentially harmful activity in federal network traffic and provides correlation and visualization of the derived data» Einstein 3.0 (CNCI n. 3) «will draw on commercial technology and specialized government technology to conduct real-time full packet inspection and threat-based decision-making on network traffic entering or leaving these Executive Branch networks. The goal of EINSTEIN 3 is to identify and characterize malicious network traffic to enhance cybersecurity analysis, situational awareness and security response».[60]

These concerns are «valid;…[the internet] security problems are analogous to having the roads overrun with bandits or the sea-lanes controlled by pirates. Under these circumstances, it is not surprising to find the government seeking to patrol the Internet, just as the nation's police and armed services have patrolled the roads or the high seas in the past.»[61] The problem is that «a system that monitors federal communications for signs of foreign intrusion will also capture all the legitimate communications that Americans have with their government.»[62]

Although the EU does not have a Cyber-security policy yet, it may follow the US example, also in relation to the talks within the EU-US WGCC. Commissioner Malmstrom has recently claimed that cybercrime and cyber-security are top priorities for the Commission, and qualified the security problem in terms of a lack of identity management: if people could be correctly identified online, abuses could be better traced afterwards.[63]

If a national security view was endorsed, the pursuit of security would entail surveillance, and privacy and data protection would be seen as the value opposed to security (despite the declarations concerning the respect of liberties and privacy), similar to, and reinforcing what is taking place in the field of broad cybercrimes. This would endanger privacy and data protection, as well as cyber-security itself. In fact, «policing the Internet, *as opposed to securing the computers that populate it*[64], may be a treacherous remedy. Will the government's monitoring tools be any more secure than the network they are trying to protect? If not, we run the risk that the surveillance facilities will be subverted or actually used against the [nation]. The security problems that plague the Internet may beset the computers that will do the policing as much as the computers being policed. If the government expands spying on the Internet without solving the underlying computer security problems, we are courting disaster.»[65]

---

59 (Pearlman, 2010); (Diffie & Landau, 2008); (The White House).

60 (The White House).

61 (Diffie & Landau, 2008), p. 3.

62 *Ibid.*

63 (Malmström, 2011).

64 Italics mine.

65 (Diffie & Landau, 2008), page 4.

b) The computer security community: de facto security and privacy integration

The underlying computer security problems are those tackled by the technical security community. In particular, its members focus on a broad variation of individual harms, such as damage to property, autonomy, privacy and productivity,[66] roughly corresponding to narrow cybercrimes (i.e. illegal access, illegal interception, data interference, system interference and misuse of devices, computer-related fraud and forgery). From a technical point of view, security is canonically[67] intended in terms of integrity, confidentiality and availability of the service. «Integrity is a degree of confidence that the data (and system) is supposed to be there, and is protected against accidental or intentional alteration without authorization…(it) is supported by well audited code, well-designed distributed systems and robust access control mechanisms. Availability means being able to use the system as anticipated.» Finally, «confidentiality refers to keeping data private. Privacy is of tantamount importance as data leaves the borders of the organization…(it) is supported by, among other things, technical tools such as encryption and access control, as well as legal protection.»[68] In other words, privacy is embedded in the concept of technical security. This is reflected in the Fair Information Practices Principles,[69] one of which is 'security of the processing operations of the personal data'.

According to the technical security community, the best strategy is pre-emption, achieved by reinforcing each node. In fact, narrow cybercrimes largely depend either on the fact that individuals' computer systems and data lack sufficient protection, such as encryption, firewalls and antivirus software, run outdated programmes exposed to bugs and exploits, or that users are unaware and vulnerable to social engineering. Also computer-related forgery and fraud could be avoided by higher protection of the individual: if the data, the system, and the communications are protected, the odds of an incident are reduced.

Accordingly, the canonical goals apply both at the end point– the individual machine – and at the systemic level – the network and its services. Both are part of CII, as defined in the introduction, namely ICT physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would seriously harm citizens, hamper the functioning of the society and governments. Therefore, in order to achieve cyber-security, intended as the policy tackling the protection of CII, one has to adopt the same preventive measures relating to narrow cybercrime, which include norms to protect…informational privacy (data protection)!

66 Ibid.

67 In practice, security is more nuanced than that, as «getting protection right…depends on several different types of processes. You have to figure out what needs protecting, and how to do it.» (Anderson R., 2008) p. 2.

68 (Friedman & West, 2010).

69 FIPPs are overarching principles of privacy that are internationally acknowledged.

Hence, by pushing for the adoption of measures that allow structural surveillance, we are both disrupting cyber-security, intended as the prevention of narrow cybercrime at a systemic level, and leading to a defeat of privacy and data protection.

4. (CYBER)SECURITY AND DATA PRIVACY: A COMPLEMENTARY GOAL

In the previous section, I attempted to demonstrate that, if one looks at the factual conditions of privacy and security in the cyber-realm, one can easily show the overlap between security and privacy/data protection. This is not to say that privacy and data protection are the key to solving the problems of cybercrime and cyber-security, but that they may be more a support than an obstacle, contrary to the zero sum game depicted by the broad cybercrime and national security communities.

Indeed, if one can say that, by applying good confidentiality and integrity measures, privacy is defended, one could also say that, by applying good privacy measures, confidentiality and integrity are attained (at least as far as the personal data part is concerned). In this case, «not only individuals, but the society is better off if privacy exists. Privacy serves collective individual and public purposes»[70] and its respect should be encouraged at all levels.

The technical approach recognises the importance of regulation for the pursuit of confidentiality. Actually, this thinking is incorporated both in EU policies (at least until recently)[71], and in privacy and data protection rules that integrate provisions contained in the proposal to a Directive on Attacks against Information Systems.[72] Data protection and privacy laws, as they currently stand, can be divided into two groups: the rules which discipline cyber-crime and security from the personal data perspective, which show 'complementarity', and the rules which impose obligations which 'contribute' to the prevention of cybercrimes and the pursuit of cyber-security.

4.1. Rules complementary to cybercrime and the pursuit of cyber-security

The first group includes the following:

- Article 16 of the Directive 95/46[73], article 5 of the e-Privacy Directive[74] on confidentiality, and to a certain extent articles 6 on traffic data and 9 on location data other than

70 (Reagan in Bennett & Raab, 2006), p. 23.

71 In the EU, cybercrime, cyber-security and data protection have been part until recently of the same 'macro-policy', namely the 'three-pronged' approach (Porcedda M. G., Data Protection and the Prevention of Cybercrime: a Dual Role for Security Policy in the EU?, 2011).

72 (European Commission, Proposal for a Directive on Attacks against Information Systems and repealing Council Framework Decision 2005/222/JHA. COM (2010) 517, 2010).

73 Directive 95/46/EC, OJ L 281, 23.11.1995, p. 31.

74 Directive 2002/58/EC, OJ L 201, 31.07.2002, p. 37.

traffic data, prohibit illegal interception of data, which is punished by article 6 of the proposed Directive on Attacks against Information Systems;

- The revised article 5.3 of the e-privacy Directive, which mandates to request the consent to install cookies, forbids illegal access to information systems, which is punished by article 3 of the proposed Directive;
- Article 13 of the e-privacy Directive proscribes spamming, which is an illegal system interference pursuant to article 4 of the proposed Directive;
- Article 24 of Directive 95/46 on sanctions is in line with both articles 9 on penalties and 11 on liability of legal persons of the proposed Directive.

The same articles also prohibit computer fraud and forgery, i.e. article 7 and 8 of the Cybercrime Convention, insofar as the data which is the object of the offence is considered personal within the meaning of article 2 of Directive 95/46/EC.

4.2. Rules contributing to the prevention of crimes and cyber-security

The rules which can contribute to the prevention of cyber-crime and the pursuit of cyber-security are the following:

- Article 17 of Directive 95/46 creates preventive measures for all offences which involve a breach of data security, as tackled by articles 3 to 6 of the proposed Directive on Attacks against Information Systems, thanks to the obligation to adopt the necessary organizational and technical measures,[75] which must be appropriate to the risks posed by the processing activity, provided these are technically and economically feasible for the controller or the processor (which must in turn be chosen in an accurate manner).
  - Examples of appropriate technical security measures are: an adequate information management system to control access to data (this includes the use of audit trails, which allow logs to be kept); the use of Privacy Enhancing Technologies (PETs) and protection against breaches, for example through the use of patches, encryption etc.; the obligation to segregate the data stored; and maintaining a person responsible for security.[76]
  - Proposed procedural measures include: obligations to audit the system (and keep audit-trails); cooperation between service providers and DPAs (allowing audit of security measures/issuance of recommendations); and a privacy/security policy expressed in clear language.[77]

Measures adopted in accordance with this article, and in particular the creation of logs and audit trails, have an additional, important effect: they are particularly valuable in case of

75 Many security risks, in fact, are caused by inappropriate internal practices (inadequate procedural and technological measures), besides external factors (OECD, 2011).

76 (Barcelo, 2009).

77 (Porcedda M. G., 2012: <http://www.springer.com/law/international/book/978-94-007-2902-5>).

an investigation, as they allow to limit the volatility of the data. The idea that security and privacy clash in the context of investigations and prosecutions is often used as an argument to reject the possibility of a reconciliation. The example mentioned suggests that, contrary to the assertion of LEAs, data protection rules are not necessarily at odds with an investigation (on cybercrime).[78]

- Article 4 of the e-privacy Directive on ensuring the security of the networks, in addition to what stated above for article 13 of the e-privacy Directive, envisages a preventive approach to system interference (article 4 of the proposed Directive), including non-commercial spamming and DDoS attacks;
- The new article 4.3 of the e-Privacy Directive on mandatory notification of data breaches is particularly important to fill the gap between misaligned incentives, i.e. the fact that those who should provide security – i.e. the producers/service providers – are not those immediately needing it (the users); the latter are often unaware of such a need or assume protection de facto.[79] The measure introduces legal incentives, i.e. the obligation to report, and social incentives, i.e. the fear of customers' loss of confidence. It also encourages the use of preventive techniques: if encryption is in place, the service provider is not obliged to report.
- The new article 5.3 has sparked a rush to compliance for a transparent use of cookies. This is helpful in preventing illegal interception (article 6 of the proposed Directive).

4.3. Revision of data protection laws and cybercrime legislation

Provided that the rules governing data protection are aligned with the technological reality, privacy and security can be integrated. Privacy and data protection in fact fill in the gap of preventive measures in cybercrime legislation, which is crucial due to the problem of attribution (provided that the coherency and certainty of law should be ensured).

The proposal for a new Regulation replacing Directive 95/46/EC, and a Directive replacing Council Framework Decision 2008/977/JHA, seem to be innovating in such a way as to ensure a continuation of this line of reasoning. This is clearly the case of the provisions relating to information security. New provisions oblige companies to step up security measures, and data controllers to notify data breaches to the DPAs and the individuals without undue delay (24 hours). This is crucial in order to allow all actors to take the necessary measures, and to allow investigation. Moreover, the proposed Regulation encourages the use of PETs, which are geared towards the prevention of privacy-related incidents. Privacy by

78 Actually, I maintain that a clash can be avoided, provided that better data protection rules in the area of police and judicial cooperation, i.e. a core-periphery approach to personal data (Scheinin, 2009), are adopted. See (Porcedda M. G., Data Protection and the Prevention of Cybercrime: a dual role for security policy in the EU?, 2011).

79 (European Data Protection Supervisor, 2010).

design,[80] whereby the respect of privacy is embedded in the very design of regulations and technologies, becomes a 'principle' of data protection. Also, the Regulation lays down rules on the procedural aspects of security, such as the obligation to have a Data Protection Officer in companies with more than 250 employees, and privacy impact assessments become mandatory in case of risky processing.

However, it will be some time before these rules become legally binding, which is why this paper focuses on the existing legal framework. Moreover, the political struggle behind the new text may water down some of its provisions; doubts in this direction have been expressed, for instance, for what concerns the proposed Directive.[81] Mixed signals are also being sent from the policy domain as to the prevailing values.[82]

5. CONCLUSION

I have tried to demonstrate that the adoption of cyber-security and cybercrime policies, one of the potential sources of highest damage to privacy and data protection when it promotes increased surveillance, actually offers a fortuitous opportunity to revive the respect of these two rights. In fact, in order to pursue cyber-security, narrow cybercrime needs to be tackled by focussing on prevention, and in particular on technical and procedural measures which enhance, or do not affect, privacy and data protection. Therefore, blanket surveillance measures and the use of informal practices (i.e. public-private partnerships) without strict guidelines, proposed by the broad cybercrime and national security communities, should be prohibited, both for the sake of security and privacy.

Logically, it could also be said that, by adopting the necessary measures to protect one's privacy, one's security is highly increased. Highly, not completely, because many actors play a role, such as the ISPs providing the networks, which are in charge of their security, and the businesses offering the market products which should be as safe as possible. In the online environment, computer security rests on the idea that responsibility is assigned in proportion to the position occupied in the chain of distribution.[83] While no one is free from obligations, those who oversee or supply should be more responsible. Clearly, distributed responsibility can be properly implemented only if it rests on the awareness of all actors.

In the EU, norms concerning the security of the network, and the related incentives, are also part of the privacy framework (the new norms on accountability laid down by the

80 (Cavoukian, 2009).

81 Remarks made at the 2012 Computers, Privacy and Data Protection conference, Brussels.

82 As far as the cyber-domain is concerned, examples include the surreptitiousness of the works of the EU-US WGCC, the Commission's 'wait and see' approach, adopted in the case of net neutrality and filtering, and even the recent cooperation with China on approximating practices on censoring illegal material on the internet. (MacNamee, 2011).

83 (OECD, 2002).

proposed Regulation reinforce this trend). As for distributed responsibility, all measures pertaining to privacy and data protection rest on the idea that data subjects are clearly and comprehensively informed, i.e. they are aware of what happens to their data, and can choose freely what level of protection they want to enjoy. However, users may not be conscious of current practices concerning their online data, and of the complementarity and overlap of best privacy and security practices. This results in partial information and misaligned incentives, and leaves room of manoeuvre for worst practices: users may be trusting services when they should not, and conceding unjustified invasions of their liberties.

If cyber-security is really at the heart of national security, it should be clear that preventive measures should be pursued and that raising awareness for privacy and security are, in the end, two sides of the same coin. The burden, following the principle of distributed responsibility, should be on those service providers which are earning the most out of users' unawareness (and insecurity), such as online entertainment service providers. More user-friendly information notices[84] would represent a first, important step, in this direction. Better responsibility at all levels also means imposing obligations on the quality of the services offered, for instance by providing real alternatives, PETs and a privacy-by-design approach (as suggested by the proposed Regulation). Privacy settings should be high by default, following behavioural economics studies according to which the way how services are presented matters.[85] More examples could be provided.

What matters here, is that the history of mankind is a continuous violation of human rights, and talk about their death, or uselessness, is instrumental to the interests of those whose businesses and activities would flourish without them. Rather than being dead, privacy and data protection are struggling to counter the attacks received. Better instrument to fight this battle, starting from privacy and data protection norms with teeth, should be provided by governments, if they do care about cyber-security.

6. BIBLIOGRAPHY

Anderson, C. (2009). *The Economics of Giving It Away.* Retrieved February, 20th, 2012 from http://online.wsj.com/article/SB123335678420235003.html.

Anderson, R. (2008). *Security Engineering. A Guide to Building Dependable Distributed Systems.* Wiley.

Anderson, R., & Murdoch, S. (2008). Tools and Technology of Internet filtering. In Ronald Deibert et al. (Eds.), *Access Denied: The Practice and Policy of Global Internet Filtering.* Cambridge: MIT Press.

84 For an encouraging initiative, see at: https://www.iubenda.com/en.

85 (OECD, 2011). Companies may be also eventually faced by consumers backlash leading to digital to resistance.

Andrews, L. (2012). *Facebook is Using You.* Retrieved March, 1st, 2012 from https://www.nytimes.com/2012/02/05/opinion/sunday/facebook-is-using-you.html?pagewanted=all.

Arthur, C. (2011). *Sony suffers second data breach with theft of 25m more user details.* Retrieved February 17th, 2012 from http://www.guardian.co.uk/technology/blog/2011/may/03/sony-data-breach-online-entertainment.

Bahls, C. (2012). *CEO Coalition to make the Internet a better place for kids.* Retrieved March, 20th, 2012 from http://www.edri.org/edrigram/number10.5/ceo-coalition-freedom-of-speech.

Barcelo, R. (2009). EU: Revision of the ePrivacy Directive. *Computer Law Review International (5)*, 129 – 160.

Bennett, C., & Raab, C. (2006). *The Governance of Privacy. Policy Instruments in a Global Perspective.* MIT PRESS.

Bilton, N. (2012). *Disruptions: So Many Apologies, So Much Data Mining.* Retrieved February, 13th, 2012 from http://bits.blogs.nytimes.com/2012/02/12/disruptions-so-many-apologies-so-much-data-mining/.

Brenner, S., & Koops, B.-J. (2006). *Cybercrime and Jurisdiction. A Global Survey.* The Hague: TMC Asser Press.

Brito, J., & Watkins, T. (2011). *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy.* Mercatus Center, George Mason University.

Brushtein, J. F. (2012). *Start-Ups Seek to Help Users Put a Price on Their Personal Data.* Retrieved, February 17th, 2012 from https://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html?_r=1&ref=technology.

Cavoukian, A. (2009). *Privacy by design…take the challenge.* Information and privacy commissioner of Ontario, Canada. Retrieved, February 20th, 2012 from http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf.

Chen, A. (2012). *Inside Facebook's Outsourced Anti-Porn and Gore Brigade, Where 'Camel Toes' are More Offensive Than 'Crushed Heads'.* Retrieved February, 18th, 2012 from http://gawker.com/5885714/inside-facebooks-outsourced-anti+porn-and-gore-brigade-where-camel-toes-are-more-offensive-than-crushed-heads.

Council Framework Decisions 2005/222/JHA of 24 February 2005 on Attacks against Information Systems. *OJ L 69*, 16.3.2005, p. 67.

Council of Europe. (1950). Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No 11 and 14, ETS No 005. Rome.

Council of Europe. (2001). Council of Europe, 'Convention on Cybercrime', European Treaty Series (ETS) no. 185. Budapest.

Council of the European Union. (2011). Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, replacing Council Framework Decision 2005/222/JHA. 11566/11. Brussels.

Darrow, B. (2012). *It's not the big data, it's the right data.* Retrieved February, 27th, 2012 from *http://gigaom.com/cloud/its-not-the-big-data-its-the-right-data/.*

Diffie, W., & Landau, S. (2008). Internet Eavesdropping: A Brave New World of Wiretapping. *Scientific American Magazine*.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L 281,* 23.11.1995, p. 31.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ L 201,* 31.07.2002, p. 37.

Eckersley, P. (2009). *How Online Tracking Companies Know Most of What You Do Online (and What Social Networks Are Doing to Help Them).* Retrieved February, 20th, 2012 from https://www.eff.org/deeplinks/2009/09/online-trackers-and-social-networks.

European Commission. (2005). Green Paper on a European Program for Critical Infrastructure Protection, COM (2005) 576 final. Brussels.

European Commission. (2010). Proposal for a Directive on Attacks against Information Systems and repealing Council Framework Decision 2005/222/JHA. COM (2010) 517 final. Brussels.

European Commission. (2012). Proposal for a Directive on the protecion of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. COM (2012) 10 final. Brussels.

European Commission. (2012). Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM (2012) 11 final. Brussels.

European Data Protection Supervisor. (2010). Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy (Opinion on Privacy By Design). Brussels.

European Data Protection Supervisor. (2011). Opinion on Net Neutrality, Traffic Management and the Protection of Privacy and Personal Data. Brussels.

European Union. (2000). Charter of Fundamental Rights of the European Union. *OJ C 364*, p. 1–22.

Friedman, A., & West, D. (2010). Privacy and Security in Cloud Computing. *Issues in Technology Innovation (3)*. The Brookings Institution.

Hasbrouk, E. (2012, March 1). *Google is now in the PNR hosting business.* Retrieved March, 15th, 2012 from http://papersplease.org/wp/2012/03/01/google-is-now-in-the-pnr-hosting-business/.

House of Lords, Science and Technology Committee. (2007). Personal Internet Security, 5th Report of Session 2006-07. London.

Juniper Networks. (2012). 2011 *Mobile Threats Report*.

Kushida, K. E. (2011). *Diffusing the Fog: Cloud Computing and Implications for Public Policy.* BRIE Working Paper 197. Berkeley.

Loayza, J. (2009). *5 Business Models for Social Media Startups.* Retrieved February, 20th, 2012 from https://mashable.com/2009/07/14/social-media-business-models/.

Lohr, S. (2012). *The Age of Big Data.* Retrieved February, 18th, 2012 from https://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?_r=1&ref=technology.

Lynn III, W. J. (2010). Defending a New Domain: the Pentagon's Cyberstrategy. *Foreign Affairs, vol. 89 (5) September/October 2010*.

MacNamee, J. (2011). *EU and China adopt harmonised approach to censorship.* Retrieved May, 20th, 2011 from http://www.edri.org/edrigram/number9.10/eu-china-censorship-internet.

Malmström, C. (2011). Speech on cybersecurity (SPEECH/11/740). *Making cyberspace more secure, Security and Defence Agenda (SDA) Cyber Security Initiative Conference on 'Defining Cyber Security'*. Brussels.

Nash, V., & Peltu, M. (2005). Rethinking Safety and Security in a Networked World: Reducing harm by Increasing Cooperation. *Forum Discussion Paper N° 6.* Oxford: Oxford Internet Institute.

Nissenbaum, H. (2007). When Computer Security meets National Security. In Jack. M. Balkin et al. (eds.), *Cybercrime. Digital Cops in a Networked Environment.* New York: New York University Press.

OECD. (2002). *Recommendation of the Council concerning Guidelines for the Security of Informations Systems and Networks – Towards a Culture of Security*.

OECD. (2011). *Thirty years after the OECD privacy guidelines.* Retrieved January, 7th, from http://www.oecd.org/dataoecd/63/56/49710223.pdf.

Ohm, P. (2010). Broken. Promises of Privacy: Responding to the Surprising Failure of Anonymization. Vol. 57, p. 1701, 2010. *University of Colorado Law Legal Studies Research Paper No. 9-12.*

Pearlman, A. R. (2010). *Federal Cybersecurity Programs, New Federal Initiatives Project.* Retrieved July, 20th, 2011 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1655105.

Peckham, M. (2011). *Sony playstation disaster: what happens next?* Retrieved January, 25th, 2012 from https://www.pcworld.com/article/226385/sonys_playstation_network_disaster_what_happens_next.html.

Porcedda, M. G. (2011). Transatlantic Approaches to Cyber-security and Cybercrime. In Patrick Pawlak (ed.), *EU-US Security and Justice Agenda in Action, Chaillot Paper n 127.* Paris: European Union Institute of Security Studies.

Porcedda, M.G. (2011). Data Protection and the Prevention of Cybercrime: a dual role for security policy in the EU? *LL.M. Thesis, Florence, European University Institute.*

Porcedda, M. G. (2012). Law Enforcement Access to Data in the Cloud: is the Data Protection Legal Framework up to the task? In Serge Gutwirth et al. (eds.), *European Data Protection: in Good Health?* Springer.

Porcedda, M.G., & Walden, I. (2011). Regulatory Challenges in a Changing Computing Environment, Working Paper. *Working paper for the Conference Law Enforcement in the Clouds: Regulatory Challenges. February 24, 2011.* Brussels: Centre de Recherche Informatique et Droit.

Ravi, K., & Shirish, N. (2012). *Big Data is the Answer. – What was the Question?* Retrieved February, 15th, 2012 from http://www.saama.com/blog/bid/76211/Big-Data-is-the-Answer-What-was-the-Question.

Rid, T. (2012). Think Again: Cyber War. *Foreing Policy*. Retrieved April 2nd, 2012 from http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,6.

Rodotà, S. (1973). *Elaboratori Elettronici e Controllo Sociale.* Bologna: Mulino.

Scarinci, D. (2012). *Security Breaches can Lead to Costly Lawsuits.* Retrieved February 20th, 2012 from http://www.businesslawnews.com/security-breaches-can-lead-to-costly-business-lawsuits/.

Scheinin, M. (2009). Terrorism and the Pull of 'Balancing' in the Name of Security. In Martin Scheinin (ed.), *Law and Security - Facing the Dilemmas.* Florence: European University Institute Working Paper N° 11.

Sommer, P., & Brown, I. (2011). *Reducing Systemic Cybersecurity Risks. OECD/IFP Project on Future Global Shocks.* Paris: OECD.

The White House. (s.d.). *The Comprehensive National Cybersecurity Initiative, National Securit Council.* Retrieved April, 15th, 2012 from http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

Thiele, M. (2012). *Big data adoption issues – What's the big deal?* Retrieved February, 27th, 2012 from http://gigaom.com/cloud/big-data-adoption-issues-whats-the-big-deal/.

United Nations. (2009). *Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes.* New York: Counter-Terrorism Implementation Task Force (CTITF).

United Nations, General Assembly. (2011). Letter to the United Nations addressed to the Secretary General, A/66/359. New York.

Williams, C. (2011). *Playstation hack: credit card data for trade.* Retrieved February, 20th, 2012 from http://www.telegraph.co.uk/technology/sony/8483183/PlayStation-hack-credit-card-data-for-sale.html.

World Economic Forum. (2012). *Big Data, Big Impact: New Possibilities for International Development.* Retrieved March, 20th, 2012 from http://www.weforum.org/reports/big-data-big-impact-new-possibilities-international-development.

CONSERVACIÓN DE DATOS E ILÍCITOS EN MATERIA DE PROPIEDAD INTELECTUAL: UNA VISIÓN CONSTITUCIONAL DE LA DIRECTIVA 2006/24

María Concepción Torres Díaz
Profesora de Derecho Constitucional de la Universidad de Alicante;
Premio Extraordinario en el Máster Oficial Sistemas y Servicios de la Sociedad de la Información, especialidad jurídica (Universidad de Valencia)

RESUMEN: El Tribunal Supremo de Suecia formuló una petición de decisión prejudicial al TJCE en el marco de un litigio entre las sociedades Bonnier Audio y otros y ePhone en relación con la oposición formulada por ePhone contra una solicitud de requerimiento judicial de revelación de información presentada por Bonnier Audio y otros, en aras de identificar a un determinado abonado. La petición pretende que el Tribunal de Justicia de las Comunidades Europeas se pronuncie sobre dos cuestiones prejudiciales. En primer lugar, si la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la presentación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones se opone a la aplicación de una disposición de derecho nacional basada en el artículo 8 de la Directiva 2004/48/CE del Parlamento Europeo y del Consejo, de 29 de abril, relativa al respeto de los derechos de propiedad intelectual, que permite que, a efectos de identificación de un abonado, se requiera en un procedimiento civil a un proveedor de acceso a Internet para que facilite al titular de un derecho de autor información relativa al abonado al que dicho proveedor de acceso asignó una dirección IP concreta, supuestamente utilizada para infringir dicho derecho. En segundo lugar, el Tribunal Supremo sueco plantea (también) si influye en la respuesta a la primera cuestión el hecho de que el Estado miembro no haya adoptado su Derecho interno a las disposiciones de la Directiva 2006/24. El planteamiento de sendas cuestiones prejudiciales resultan relevantes desde el punto de vista constitucional teniendo en cuenta los derechos susceptibles de verse afectados –a saber– intimidad personal, protección de datos, derechos de autor y, por extrapolación, secreto de las comunicaciones –todo ello en relación con la conservación de datos. Cuestiones que no son baladíes teniendo en cuenta las críticas que en su día suscitó la Directiva 2006/24. Críticas que supusieron un profundo cambio en los principios generales en materia de protección de datos y de secreto de las comunicaciones. Pero críticas que –al fin y al cabo– fueron justificadas por esa finalidad de garantizar que los datos conservados por los operadores estuvieran disponibles para las autoridades competentes con fines de investigación, detección y enjuiciamiento de delitos graves, esto es, estuvieran disponibles para luchar contra la criminalidad organizada y el terrorismo.

PALABRAS CLAVE: derechos de autor, conservación de datos, intimidad personal y derechos conexos, análisis constitucional.

1. PLANTEAMIENTO GENERAL

El Tribunal Supremo de Suecia (Högsta domstolen) formuló una petición de decisión prejudicial al TJCE en el marco de un litigio entre las sociedades Bonnier Audio y otros (Bonnier Audio AB, Earbooks AB, Norstedts Förlagsagrupp AB, Piratförlaget Aktiebolag

y Storyside AB) y ePhone en relación con la oposición formulada por ePhone contra una solicitud de requerimiento judicial de revelación de información presentada por Bonnier Audio y otros, en aras de identificar a un determinado abonado. La petición pretende que el Tribunal de Justicia de las Comunidades Europeas se pronuncie sobre dos cuestiones prejudiciales. En primer lugar, si la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la presentación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones se opone a la aplicación de una disposición de derecho nacional basada en el artículo 8 de la Directiva 2004/48/CE del Parlamento Europeo y del Consejo, de 29 de abril, relativa al respeto de los derechos de propiedad intelectual, que permite que, a efectos de identificación de un abonado, se requiera en un procedimiento civil a un proveedor de acceso a Internet para que facilite al titular de un derecho de autor información relativa al abonado al que dicho proveedor de acceso asignó una dirección IP concreta, supuestamente utilizada para infringir dicho derecho. En segundo lugar, el Tribunal Supremo sueco plantea (también) si influye en la respuesta a la primera cuestión el hecho de que el Estado miembro no haya adoptado su Derecho interno a las disposiciones de la Directiva 2006/24. El planteamiento de sendas cuestiones prejudiciales resulta relevante desde el punto de vista constitucional teniendo en cuenta los derechos susceptibles de verse afectados –a saber– intimidad personal, protección de datos, derechos de autor y, por extrapolación, secreto de las comunicaciones –todo ello en relación con la conservación de datos. Cuestiones que no son baladíes teniendo en cuenta las críticas que en su día suscitó la Directiva 2006/24. Críticas que supusieron un profundo cambio en los principios generales en materia de protección de datos y de secreto de las comunicaciones. Pero críticas que –al fin y al cabo– fueron justificadas por esa finalidad de garantizar que los datos conservados por los operadores estuvieran disponibles para las autoridades competentes con fines de investigación, detección y enjuiciamiento de delitos graves, esto es, estuvieran disponibles para luchar contra la criminalidad organizada y el terrorismo.

Partiendo de las anteriores consideraciones la presente comunicación pretende reflexionar sobre una serie de cuestiones: ¿Qué cabe entender por delitos graves a tenor de la Directiva 2006/24? ¿La infracción de derechos de propiedad intelectual entrarían dentro de esa conceptuación? ¿Quiénes son las autoridades competentes a las que alude la Directiva 2006/24? ¿Estaría justificado que en el marco de un procedimiento civil se requiera a un proveedor de acceso que facilite a un titular de derechos de autor los datos de identificación de un abonado? ¿Estaría justificada la aplicación de la Directiva 2006/24 en el caso planteado teniendo en cuenta que las dudas surgen en el marco de un litigio cuya protección es esencialmente civil o de derecho privado? ¿Qué riesgos conllevaría –desde el punto de vista de los derechos fundamentales– la extensión y/o generalización a los litigios civiles de la aplicación de una norma que nació en el seno de la lucha antiterrorista? Y es que –pendientes de la sentencia que (en su día) falle el TJCE– son muchas las dudas que suscita esta cuestión, máxime cuando se advierte que la Directiva 2006/24 puede ser utilizada para perseguir ilícitos de propiedad intelectual que exceden –y mucho– de los fines previstos en la mentada Directiva.

2. APROXIMACIÓN A LAS DIRECTIVAS 95/46 Y 2002/58

2.1. Consideraciones a la Directiva 95/46

Antes de entrar a analizar propiamente las Directivas 2006/24/CE y 2004/48/CE considero oportuno realizar algunas consideraciones generales a la Directiva 95/46/CE[1] del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Y es que la Directiva referenciada tiene como objeto –a tenor de lo dispuesto en su artículo 1– que los Estados miembros garanticen la protección de las libertades y los derechos fundamentales de las personas físicas y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. La Directiva recoge una serie de definiciones como las de datos de carácter personal, tratamiento de datos personales, fichero de datos personales, responsable del tratamiento, encargado de tratamiento, tercero, destinatario y consentimiento del interesado. Su ámbito de aplicación está recogido en su artículo 3 cuando señala que «Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero». A sensu contrario, el párrafo 2 de dicho precepto precisa que las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario como el tratamiento de datos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal, así como las actividades efectuadas por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. La Directiva recoge una serie de principios relativos a la calidad de los datos que es preciso tener en cuenta. Entre esos principios –precisa– que los datos deben ser tratados de manera leal y lícita, deben ser recogidos con fines determinados, explícitos y legítimos de tal forma que no sean tratados posteriormente de manera incompatible con dichos fines, deben ser exactos y deben estar actualizados, además, deben conservarse de tal forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se tratan ulteriormente. Junto a estos principios la Directiva alude (también) a una serie de principios relativos a la legitimación del tratamiento de datos. Su artículo 7 dispone que los Estados miembros dispondrán que el tratamiento de datos sólo puede efectuarse si el interesado ha dado su consentimiento de forma inequívoca, si es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, si es necesario

1 Véase la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Puede consultarse en la siguiente dirección url: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:ES:PDF, (fecha de consulta: 15/11/2011). Véase (también) la LO 15/1999, de 13 de diciembre en la siguiente dirección url: http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf, (fecha de consulta: 15/11/2011).

para el cumplimiento de una obligación jurídica, si es necesario para proteger el interés vital del interesado, si es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero o a quien se comuniquen los datos o, por último, si es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos. La Directiva recoge el derecho de información al interesado tanto cuando los datos se hayan recabado del propio interesado como cuando se hayan recabado de terceros. Asimismo recoge el derecho de oposición del interesado así como aspectos relacionados con la confidencialidad y la seguridad en el tratamiento de datos personales. A los objetos de esta comunicación conviene resaltar como la Directiva 95/46/CE obliga a los Estados miembros a garantizar la protección de los derechos y libertades de las personas físicas en relación con el tratamiento de datos personales estableciendo principios rectores que determinan la legalidad de dicho tratamiento.

2.2. Consideraciones a la Directiva 2002/58

La Directiva 2002/58/CE[2] del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) tiene como objetivo garantizar un nivel equivalente de protección de las libertades y derechos fundamentales y, en particular, el derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas. A los objetos de esta comunicación conviene prestar especial atención a la dicción literal del artículo 5.1 de la Directiva referenciada. Precepto que dispone textualmente,

> «Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad».

De la dicción literal del precepto extractado se observa como las únicas excepciones al principio de confidencialidad son las que se aplican a favor de las personas autorizadas legalmente, en el sentido del artículo 15, apartado 1 y las relativas al almacenamiento técnico

2 Véase la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Puede consultarse en la siguiente dirección url: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:ES:PDF, (fecha de consulta: 12/10/2011).

necesario para la conducción de una comunicación. Con respecto al apartado 1 del artículo 15 cabe señalar como dispone textualmente,

> «Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE. Para ello, los Estados miembros podrán adoptar, entre otras medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión».

Por su parte el apartado 1 del artículo 6 de la Directiva referenciada prevé que los datos de tráfico almacenados deberán eliminarse o hacerse anónimos cuando ya no sean necesarios a los efectos de la transmisión de una comunicación, sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 de dicho artículo y en el artículo 15, apartado 1 de dicha Directiva. Señala textualmente el apartado 1 del artículo 6,

> «Sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 del presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sean necesario a los efectos de la transmisión de una comunicación».

Partiendo de las anteriores consideraciones, y en virtud de lo expuesto, cabe colegir que los Estados miembros podrán adoptar medidas legales para limitar el alcance de la obligación de garantizar la confidencialidad de los datos de tráfico cuando tal limitación constituya una medida necesaria, proporcionada y apropiada, en una sociedad democrática, para proteger la seguridad nacional (defensa y seguridad pública), la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas[3].

3. APROXIMACIÓN A LA DIRECTIVA 2004/48/CE

La Directiva 2004/48/CE[4] del Parlamento Europeo y del Consejo de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual recoge una serie de considerandos de especial interés a los objetos de la presente comunicación. Seña-

3 Véase el apartado 1 del artículo 13 de la Directiva 95/46.

4 Véase la Directiva 2004/48/CE del Parlamento Europeo y del Consejo de 29 de abril de 2004, relativa al respecto de los derechos de propiedad intelectual. Puede consultarse en la siguiente dirección url: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:157:0045:0086:ES:PDF, (fecha de consulta: 22/10/2011).

la –en su considerando primero– como la realización del mercado interior ha supuesto la eliminación de las restricciones a la libre circulación así como la eliminación de las distorsiones de la competencia, al tiempo que se crea un entorno favorable a la innovación y la inversión. En este contexto, la protección de la propiedad intelectual resulta imprescindible no sólo para la promoción de la innovación y de la creación, sino también para el desarrollo del empleo y la competitividad. En la misma línea se pronuncia el considerando segundo cuando resalta como la protección de la propiedad intelectual debe permitir que el inventor o creador obtenga un beneficio legítimo de su invención o creación. En este sentido, se hace preciso garantizar una difusión amplia de las obras, ideas y conocimientos nuevos, no debiendo ser un obstáculo para la libertad de expresión, para la libre circulación de la información, ni para la protección de los datos personales, inclusive en Internet. No obstante matiza –el considerando tercero– que «sin medios eficaces de tutela[5] de los derechos de propiedad intelectual, la innovación y la creación se desincentivan y las inversiones se reducen. Por consiguiente, es preciso garantizar que el Derecho sustantivo de propiedad intelectual, que actualmente forma parte en gran medida del acervo comunitario, se aplique de manera efectiva en la Comunidad». Especial atención cabe prestar al considerando número diez. Considerando que recoge el objetivo de la presente Directiva y señala que no es otro que «aproximar dichas legislaciones [las legislaciones de los Estados miembros] para garantizar un nivel de protección de la propiedad intelectual elevado, equivalente y homogéneo en el mercado interior». Se observa como el objeto no es establecer normas armonizadas sobre cooperación judicial, competencia judicial, reconocimiento y ejecución de las decisiones en materia civil y mercantil, ni tratar de la legislación aplicable, sino que su objeto queda delimitado en su artículo 1 cuando señala como la presente Directiva «se refiere a las medidas, procedimientos y recursos necesarios para garantizar el respeto de los derechos de propiedad intelectual». El artículo 2 de la Directiva alude al ámbito de aplicación y precisa –en su apartado 2– que afectará a los derechos de autor sin perjuicio de disposiciones específicas relativas al respeto de los derechos y a las excepciones establecidas por la legislación comunitaria, en particular en la Directiva 91/250/CEE, concretamente en su artículo 7, o en la Directiva 2001/29/CE, concretamente en sus artículos 2 a 6 y 8. Por su parte la Directiva no afectará –según lo recogido en el apartado 3 del artículo 2– a las disposiciones comunitarias que regulan el Derecho sustantivo de propiedad intelectual, la Directiva 95/46/CE, la Directiva 1999/93/CE y la Directiva 2000/31/CE, en general, y los artículos 12 a 15 de esta última en particular. Tampoco afectará a las obligaciones internacionales de los Estados miembros ni a ninguna disposición nacional de los Estados miembros relativa a los procedimientos o sanciones penales con respecto a las infracciones de los derechos

5 Sobre los medios de tutela de los derechos de propiedad intelectual habrá que estar a lo dispuesto en los convenios internacionales en materia de propiedad intelectual tales como el Convenio de París para la protección de la propiedad industrial, el Convenio de Berna para la protección de las obras literarias y artísticas y la Convención de Roma sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión.

de propiedad intelectual. El artículo 3 recoge una serie de disposiciones generales entre las que cabe destacar una obligación general en la que se insta a los Estados miembros a que establezcan las medidas, procedimientos y recursos necesarios para garantizar el respeto de los derechos de propiedad intelectual a los que se refiere la presente Directiva. El precepto precisa que dichas medidas serán justas y equitativas así como efectivas, proporcionadas y disuasorias y se aplicarán del tal modo que se evite la creación de obstáculos al comercio legítimo y se ofrezcan salvaguardias contra su abuso.

Sin perjuicio de lo expuesto conviene prestar especial atención al artículo 8 en donde se recoge el derecho a la información. El párrafo 1 de dicho precepto dispone textualmente,

> «Los Estados miembros garantizarán que, en el contexto de los procedimientos relativos a una infracción de un derecho de propiedad intelectual y en respuesta a una petición justificada y proporcionada del demandante, las autoridades judiciales competentes puedan ordenar que faciliten datos sobre el origen y las redes de distribución de las mercancías o servicios que infringen un derecho de propiedad intelectual el infractor o cualquier persona que: a) haya sido hallada en posesión de las mercancías litigiosas a escala comercial; b) haya sido hallada utilizando servicios litigiosos a escala comercial; c) haya sido hallada prestando a escala comercial servicios utilizados en las actividades infractoras o d) haya sido designada por la persona a que se refieren las letras a), b) o c) como implicada en la producción, fabricación o distribución de dichas mercancías o en la prestación de dichos servicios».

Por su parte el párrafo 2 del mismo precepto recoge que los datos a los que se refiere el apartado 1 incluirán los nombres y direcciones de los productores, fabricantes, distribuidores, suministradores y otros poseedores anteriores de las mercancías o servicios, así como de los mayoristas y minoristas destinatarios asi como información –en su caso– sobre las cantidades producidas, fabricadas, entregadas, recibidas o encargadas, así como sobre el precio obtenido por las mercancías o servicios de que se trate.

A los objetos de la presente comunicación –y por lo que respecta a la protección de datos– conviene significar el contenido del párrafo 3 del artículo 8. Según esta disposición, los apartados 1 y 2 antes referenciados, que regulan el acceso a datos que puedan estar relacionados con infracciones a un derecho de propiedad intelectual, se aplicarán sin perjuicio de otras disposiciones legales y reglamentarias que regulen el tratamiento de datos personales. Dispone textualmente,

> «Los apartados 1 y 2 se aplicarán sin perjuicio de otras disposiones legales que: a) concedan al titular derechos de información más amplios; b) regulen la utilización de los datos que se comuniquen con arreglo al presente artículo en procedimientos civiles o penales; c) regulen la responsabilidad por abuso del derecho de información; d) ofrezcan la posibilidad de negarse a facilitar datos que obliguen a la persona a la que se refiere el apartado 1 a admitir su propia participación o la de sus parientes cercanos en una infracción de un derecho de propiedad intelectual, o e) rijan la protección de la confidencialidad de las fuentes de información o el tratamiento de los datos personales».

De lo expuesto se observa como la Directiva indica que hay que respetar las disposiciones legales y reglamentarias que regulan el tratamiento de datos personales pero no especifica que datos pueden ser conservados, ni la finalidad de su conservación, ni su duración o las personas que pueden acceder a los mismos en caso de infracción de derechos de propiedad intelectual. Por tanto, estamos ante una omisión importante teniendo en cuenta la cuestión suscitada en la cuestión prejudicial planteada.

4. APROXIMACIÓN A LA DIRECTIVA 2006/24/CE

Con respecto a la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones tiene como cometido - según su artículo 1 apartado 1,

> «(...) armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro».

Su párrafo segundo señala cuáles son los datos sobre los que se aplicará la Directiva siendo éstos los datos de tráfico y de localización sobre personas físicas y jurídicas y los datos relacionados necesarios para identificar al abonado o usuario registrado. No obstante, precisa el precepto que no se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas.

Partiendo de la dicción literal del precepto anteriormente reseñado resulta importante aludir a los distintos considerandos que se incluyen y que tratan de justificar la aprobación de la misma. El considerando primero alude a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos. El considerando segundo se hace eco de la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. También es importante tener en cuenta las Conclusiones del Consejo de Justicia e Interior de 19 de diciembre de 2002 en donde se destaca la importancia de los datos relativos al uso de las comunicaciones electrónicas como instrumentos para la prevención, investigación, detección y enjuiciamiento de delitos. Junto a esto, la Declaración sobre la lucha contra el terrorismo[6], adoptada por el Consejo Europeo el 25 de marzo de 2004, tuvo entre otros objetivos examinar las medidas para establecer normas sobre la conservación por los prestadores de servicios de datos de tráfico de las comunicaciones.

Siguiendo con el contenido de la Directiva 2006/24/CE conviene precisar como resalta la importancia de los datos de tráfico y localización para la investigación, detección y enjuiciamiento de delitos, según demuestra la investigación y la experiencia práctica de varios Estados miembros, existiendo la necesidad de asegurar a escala europea que los datos generados o tratados, en el marco de la prestación de servicios de comunicaciones, por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública

6 Vease la Declaración sobre la lucha contra el terrorismo, adoptada por el Consejo Europeo, de 25 de marzo de 2004. Puede consultarse en la siguiente dirección url: http://www.realinstitutoelcano.org/especiales/atentados/docs/declaracterrorUE25304.pdf, (fecha de consulta: 22/11/2011).

de comunicaciones se conserven durante un determinado período de tiempo con arreglo a las condiciones establecidas en la presente Directiva. En vista de lo expuesto, queda patente la importancia de la conservación de datos en las comunicaciones electrónicas en vista de futuras investigaciones y enjuiciamiento de delitos.

Partiendo de las consideraciones anteriores conviene resaltar como los objetivos de la Directiva 2006/24/CE son, por un lado, armonizar las obligaciones de los proveedores de conservar determinados datos en el ámbito europeo y, por otro, asegurar que éstos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la normativa nacional de cada Estado miembro. Ahora bien ¿qué cabría entender por delitos graves? Según señala la Directiva dentro de la conceptuación de delitos graves se encuentran el terrorismo y la delincuencia organizada. Esta precisión no es baladí si se tiene en cuenta los riesgos para la privacidad y para el secreto de las comunicaciones que las medidas establecidas en la Directiva comentada son susceptibles de generar. En este sentido resulta importante aludir también a la Carta Europea de Derechos Humanos, concretamente a sus artículos. 7 y 8, en donde se reconocen los derechos de respeto de la vida privada y familiar y de protección de datos de carácter personal.

En cuanto al articulado de la Directiva 2006/24/CE cabe señalar que está formada por 17 artículos. El artículo 1 enmarca el objeto y el ámbito de aplicación de la Directiva. El artículo 2 recoge una serie de definiciones importantes, el artículo 3 delimita la obligación de conservar datos. El artículo 4 regula el acceso a los datos, esto es, quiénes serán los autorizados para acceder a los mismos. El artículo 5 recoge el elenco de datos que deben conservarse. El artículo 6 determina el lapso de tiempo en el que deberán ser conservados los datos. El artículo 7 recoge una serie de principios mínimos de seguridad que deberán observar los proveedores de servicios de comunicaciones electrónicas de acceso público. El artículo 8 regula los requisitos de almacenamiento para los datos conservados. El artículo 9 regula las autoridades de control, etc. Sin ánimo de profundizar en el articulado de la Directiva –a los objetos de esta comunicación– conviene apuntar una serie de críticas en cuanto al profundo cambio en los principios generales en materia de protección de datos y secreto de las comunicaciones que comporta. Cambios que tienen como finalidad garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves. A tenor de lo expuesto, se observa como se concede a los Estados amplias facultades de control que han sido ampliamente criticadas por las instancias que velan por la adecuada protección de datos personales ya que supone contravenir los principios, hasta el momento asentados, sobre esta materia. Todo ello fue fruto de la preocupación por la seguridad y la necesidad de dotar a los Estados de los máximos instrumentos para luchar contra el terrorismo. Como señala VILASAU[7],

> «(...) la adopción de una medida sobre retención de datos ha comportado la valoración de distintos intereses en juego contrapuestos. Frente al interés de las autoridades en la retención para luchar de forma más eficaz contra el terrorismo y otras formas de delincuencia organizada, se halla el derecho

7 VILASAU, M. (2006). La Directiva 2006/24/CE sobre conservación de datos de tráfico en las comunicaciones electrónicas: seguridad v. privacidad. IDP, Revista de Internet, Derecho y Política, nº 3, UOC. Recuperado fecha de consulta 10/05/2007, en http://www.uoc.edu/ojs/index.php/idp/article/view/398.

> fundamental de los ciudadanos a la protección de sus datos. Además, hay que añadir los intereses de los proveedores de servicios de comunicaciones electrónicas en que no les atribuyen más cargas económicas derivadas de las nuevas obligaciones».

De lo expuesto hasta este momento cabría colegir que la finalidad de la Directiva 2006/24/CE queda bastante clara. Una finalidad que –a priori– quedaría fuera de aplicarse al caso objeto de comentario. Y es que conviene recordar que según su artículo 1 –anteriormente citado– busca garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro. Por el contrario, el asunto principal del caso planteado es un procedimiento civil y los datos no los solicita a una autoridad nacional sino a unos particulares.

5. ANÁLISIS CONSTITUCIONAL Y DERECHOS AFECTADOS

Partiendo de las consideraciones expuestas en los apartados anteriores resulta factible realizar algunas consideraciones desde el punto de vista constitucional. Y es que los derechos susceptibles de verse afectados invitan a una reflexión desde esta óptica de análisis. En este sentido, en cuanto a derechos afectados cabría señalar el derecho a la intimidad y la protección de datos, el derecho al secreto de las comunicaciones sin olvidar los derechos de autor. Derechos –todos ellos– de relevancia constitucional que derivan de su propia ubicación sistemática en nuestra Carta Magna. Ubicación que les otorga una serie de características propias y unas garantías de tutela y protección reforzadas[8]. Y es que hablamos de derechos recogidos en la sección 1ª del capítulo 2º del Título I de la Constitución española. Derechos dotados de una doble dimensión subjetiva[9] y objetiva[10] y derechos cuya constitucionalización les hace tributarios de una serie de caracteres como su aplicabilidad directa, su vinculación a todos los poderes públicos y a la ciudadanía[11] y su protección jurisdiccional.

Con respecto al derecho a la intimidad está recogido en el artículo 18.1 CE junto con el derecho al honor y la propia imagen. Desde el punto de vista constitucional se busca resguardar de la acción y el conocimiento ajenos un ámbito propio y reservado de cada sujeto, que se considera necesario para mantener una calidad mínima de vida humana. Por su parte, el derecho a la protección de datos se encuentra en el apartado 4 del artículo 18 CE. Se ha configurado como un derecho autónomo –a pesar de que esta cuestión ha sido y es ampliamente debatida– que otorga a sus titulares un poder de disposición sobre los propios datos. El secreto de las co-

8 Sobre las garantías veáse el artículo 53 CE.

9 Con respecto a la dimensión subjetiva de los derechos fundamentales y/o constitucionales deriva de su relación con la dignidad humana (art. 10.1 CE) y se concretan en facultades que garantizan un ámbito libre de intervención y actuación frente a eventuales injerencias o intromisiones.

10 Con respecto a la dimensión objetiva cabría precisar que genera la obligación de los poderes públicos de contribuir a la efectividad de los derechos en su desarrollo, interpretación y aplicación.

11 Véase el artículo 9.1 de la Constitución española. Dicho precepto dispone *«Los ciudadanos y los poderes públicos están sujetos a la Constitución y al resto del ordenamiento jurídico».*

municaciones[12] protege tanto el proceso de comunicación como el contenido de la misma. Partiendo de esta definición se puede señalar que el secreto de las comunicaciones garantiza tanto el proceso de comunicación como el conocimiento antijurídico de las comunicaciones ajenas. Además, el derecho también protege la identidad subjetiva de los interlocutores. Con respecto a los derechos de autor véase lo preceptuado en el artículo 20.1.b) cuando señala «Se reconocen y protegen los derechos (…) b) A la producción y creación literaria, artística, científica y técnica (...)». De la dicción literal de este precepto cabría colegir que se reconoce el derecho a crear libremente en el ámbito artístico y a producir en el ámbio científico. También protege el objeto del proceso creador y el derecho a difundir el contenido de lo creado y/o producido.

A tenor de todo lo anterior y teniendo en cuenta la petición de decisión prejudicial formulada ante el TJCE por el Tribunal Supremo de Suecia en el marco del litigio entre las sociedades Bonnier Audio y otros y ePhone –y desde el ámbito constitucional– es necesario traer a colación referentes importantes en aras de intentar delimitar cuál es el escenario del que partimos y cuál es el escenario al que se podría llegar. Referentes como la STEDH de 2 de agosto de 1984, caso Malone, en donde el TEDH reconoce expresamente la posibilidad de que el artículo 8 de la Convención Europea de Derechos Humanos pueda resultar vulnerado por el empleo de un artificio técnico –comptage– que permite registrar cuáles han sido los números telefónicos marcados sobre un determinado aparato aunque no el contenido de la comunicación misma. Referentes como la STJUE, de 29 de enero de 2008, caso Promusicae, en donde el Tribunal de Justicia de la Unión Europea declaró que no existe una obligación a los Estados miembros de imponer el deber de comunicar datos personales con objeto de garantizar la protección efectiva de los derechos de autor en el marco de un procedimiento civil. No obstante, conviene significar como el TJCE instó a los Estados miembros a que adaptaran su ordenamiento jurídico interno en aras de garantizar un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario. El TJCE precisó –además– que son las autoridades y órganos jurisdiccionales de los Estados miembros a los que compete interpretar el derecho nacional de conformidad con las Directivas comunitarias. Interpretación que debe evitar conflictos entre derechos fundamentales y principios generales de Derecho comunitario, entre los que cita el principio de proporcionalidad[13]. En cualquier caso –a los objetos de esta comunicación– resulta interesante señalar como el TJCE ve compatible con el Derecho comunitario que los Estados miembros excluyan la comunicación de datos de tráfico personales para la persecución

12 Sobre el secreto de las comunicaciones veáse PULIDO QUECEDO, M. (2006). *La noción de «secreto de las comunicaciones postales» ex art. 18.3 CE*. Repertorio Aranzadi del Tribunal Constitucional, núm. 16/2006, Pamplona. Véase también NARVÁEZ RODRÍGUEZ, A. (1999). *Intervenciones telefónicas*. En Repertorio Aranzadi del Tribunal Constitucional, vol II, Pamplona: Aranzadi. Sobre esta materia resulta interesante (también) JIMÉNEZ CAMPOS, J. (1987). *La garantía constitucional del secreto de las comunicaciones.* En Revista Española de Derecho Constitucional, nº 20, pp. 42 y ss.

13 Sobre la proporcionalidad resulta interesante citar la Sentencia del Tribunal Constitucional Alemán de 2 de marzo de 2010 en donde el máximo intérprete constitucional declaró inconstitucional la Ley de conservación de datos por la que se transpone la Directiva 2006/24/CE. Sobre la proporcionalidad resulta interesante – entre otros – el FJ 5 de la STC 66/1995, de 8 de mayo.

por vía civil de infracciones de derecho de autor. Y es que no podemos olvidar que esos datos de tráfico son susceptibles de socavar derechos fundamentales como la intimidad, protección de datos y el secreto de las comunicaciones. Vulneración que se produciría para resolver cuestiones civiles –caso de Promusicae– en donde estamos ante un intercambio de ficheros de música a través de redes p2p sin ánimo de lucro que no constituyen delito.

Junto a los referentes anteriores conviene señalar (también) las sentencias de nuestro intérprete constitucional sobre el valor jurídico de las interceptaciones de las comunicaciones cuando éstas consisten en indagar en los listados de llamadas telefónicas a través de las compañías telefónicas o mediante el acceso a los registros de llamadas de los móviles. Y es que el Tribunal Constitucional en una reiterada jurisprudencia[14] ha venido señalando que el derecho al secreto de las comunicaciones como derecho fundamental consagra la libertad de las comunicaciones y su secreto, estableciendo –en este último sentido– la interdicción de la interceptación o del conocimiento antijurídico de las comunicaciones ajenas. Por tanto, el bien jurídico protegido es la libertad de las comunicaciones. Libertad que se vería socavada tanto si se produjera una interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje con conocimiento o no del mismo, o captación, de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado. Además, conviene precisar como la delimitación jurídica del 'secreto de las comunicaciones' cubre no sólo el contenido de la comunicación sino también la identidad subjetiva de los interlocutores, de ahí que se haya afirmado que la entrega de los listados de llamadas telefónicas por las compañías telefónicas a la policía, sin consentimiento del titular del teléfono, requiera resolución judicial y lo mismo cabría apuntar con respecto al acceso al registro de llamadas memorizadas en el terminal de un móvil.

Otro aspecto importante sobre el que prestar especial atención –al hilo de la cuestión prejudicial planteada por el Tribunal Supremo de Suecia– es el relativo a la relevancia jurídica del número IP un aspecto no menor y que obliga a tener en cuenta tanto la Consulta 1/1999 de la Fiscalía General del Estado como los Informes de la Agencia Española de Protección de Datos sobre direcciones IP[15] y sobre cesión de datos a las Fuerzas y Cuerpos de Seguridad del Estado[16], sin olvidar los documentos de Trabajo del GdT 29 entre los que destaca el Documento de Trabajo sobre Privacidad en Internet. Y es que un análisis de los mismos determina que la consideración de la dirección IP como dato personal obliga a que la interceptación de los datos de tráfico requiera de un abordaje específico dado su carácter sensible. Un abordaje que entronca directamente en nuestro ordenamiento jurídico interno con la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Norma que contiene un objeto limitado en cuanto a la regulación

14 Véase –entre otras– la STC 230/2007, de 5 de noviembre de 2007. Interesantes resultan también la STC 70/2002, de 3 de abril de 2002 y la STC 114/1984, de 29 de noviembre de 1984.

15 Véase –entre otros– el Informe 327/2003, de la Agencia Española de Protección de Datos, sobre carácter de dato personal de la dirección IP.

16 Véase el Informe 213/2004, de la Agencia Española de Protección de Datos, sobre cesión de la dirección IP a las Fuerzas y Cuerpos de Seguridad.

de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales. Partiendo de ese objeto limitado que recoge la Ley 25/2007 en su artículo 1 –que supone la transposición de la Directiva 2006/24/CE– resulta cuestionable que se obligue a un proveedor de acceso a Internet para que facilite al titular de un derecho de autor información relativa al abonado al que dicho proveedor asignó una dirección IP concreta.

6. CONSIDERACIONES FINALES

Teniendo en cuenta las consideraciones planteadas al inicio de la presente comunicación y lo dispuesto en los distintos puntos desarrollados a lo largo de la misma cabría resaltar esa visión constitucional que se extrapola de las cuestiones planteadas. Visión que viene determinada por los propios derechos susceptibles de verse afectados y que han sido objeto de planteamiento en la cuestión prejudicial ante el TJCE por parte del Tribunal Supremo de Suecia en el marco del litigio entre las sociedades Bonnier Audio y otros y ePhone en relación con la oposición formulada por ePhone contra una solicitud de requerimiento judicial de revelación de información presentada por Bonnier Audio y otros, en aras de identificar a un determinado abonado. Y es que a tenor del contenido de las Directivas objeto de análisis –a saber– la Directiva 2006/24/CE así como la Directiva 2004/48/CE –parece difícil que pudiera extrapolarse una cierta obligación por parte de ePhone de revelar los datos de identificación del abonado ante el requerimiento realizado por Bonnier y otros en el marco de un procedimiento civil. Cuestión distinta sería que esa cesión de datos se enmarcara en una investigación, detección o enjuiciamiento de delitos graves. No obstante, la cuestión no resulta sencilla máxime teniendo en cuenta el desarrollo normativo interno en Suecia del artículo 8 de la Directiva 2004/48/CE que permite que a efectos de identificación de un abonado (efectivamente) se requiera, en un procedimiento civil, a un proveedor de acceso a Internet para que facilite al titular de un derecho de autor información relativa al abonado al que dicho proveedor de acceso asignó una dirección IP. Desarrollo normativo que –a mi juicio– colisiona con el contenido de la Directiva 2006/24/CE de conservación de datos. Directiva que nació con una finalidad muy determinada que justifica –no sin ciertas dudas en materia de una posible vulneración del derecho al secreto de las comunicaciones– la conservación de datos por parte de los proveedores de servicios de la sociedad de la información con fines de investigación, detección y enjuiciamiento de delitos graves. En cualquier caso, la cuestión está sub júdice[17] y habrá que estar a la resolución del TJCE en aras de analizar los

17 Conviene reseñar que una vez finalizado el texto de la comunicación se ha hecho pública la Sentencia del Tribunal de Justicia de 19 de abril de 2012 («Derechos de autor y derechos afines –Tratamiento de datos por Internet –Vulneración de un derecho exclusivo – Audiolibros a los que se posibilita el acceso gracias a un servidor FTP a través de Internet mediante una dirección IP proporcionada por el

argumentos jurídicos que fundamenten una solución al caso planteado y que nos permitan atisbar hacia dónde se camina en esta materia.

7. BIBLIOGRAFÍA

Arenas Ramiro, M. (2007). El derecho a la protección de datos personales como garantías de las libertades de expresión e información. En COTINO HUESO, L. (coord.). Libertad en Internet. La red y las libertades de expresión e información. Valencia: Tirant Lo Blanch.

Consulta 1/1999, de la Fiscalía General del Estado, de 22 de enero de 1999.

Documentos de Trabajo del GdT 29 sobre Privacidad en Internet, de 21 de noviembre de 2000.

Gómez Sánchez, Y. (2005). Derecho Constitucional Europeo. Derechos y libertades. Madrid: Sanz y Torres.

Informe 327/2003, de la Agencia Española de Protección de Datos, sobre carácter de dato personal de la dirección IP.

Informe 213/2004, de la Agencia Española de Protección de Datos, sobre cesión de la dirección IP a las Fuerzas y Cuerpos de Seguridad.

---

operador de Internet – Requerimiento al operador de Internet para que facilite el nombre y la dirección del usuario de dirección IP») en el asunto C-461/10, Bonnier Audio AB y otros frente a Perfect Communication Sweden AB. La sentencia analiza las directivas referenciadas en esta comunicación y declara que la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, debe interpretarse en el sentido de que no se opone a la aplicación de una normativa nacional, basada en el artículo 8 de la Directiva 2004/48 del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual, que, a efectos de la identificación del abonado a Internet o de un usuario de Internet, permite que se requiera judicialmente a un proveedor de acceso a Internet para que comunique al titular de un derecho de autor la identidad del abonado a quien se ha asignado una determinada dirección IP que supuestamente ha servido para la vulneración de dicho derecho, puesto que tal normativa es ajena al ámbito de aplicación *ratione materiae* de la Directiva 2006/24. Además, precisa el TJCE que carece de intéres en el procedimiento principal el hecho de que el Estado miembro interesado no haya adaptado aún su ordenamiento interno a la Directiva 2006/24. El TJCE precisa que las Directivas 2002/58 y 2004/48 deben interpretarse en el sentido de que no se oponen a una normativa nacional que permita al órgano jurisdiccional nacional que conozca de una acción por la que se solicite un requerimiento judicial de comunicación de datos de carácter personal ponderar, en función de las circunstancias de cada caso y con la debida observancia de las exigencias derivadas del principio de proporcionalidad. Se observa como la decisión del TJCE difiere de las consideraciones finales plasmadas en esta comunicación. Lo que – sin duda – nos invita a reflexionar sobre esa deriva que se advierte cuando se extiende la aplicación de unas medidas nacidas en el seno de la lucha antiterrorista a litigios de naturaleza civil. Y es que ¿no estaremos ante nuevas formas de control estatal?

Jiménez Campos, J. (1987). La garantía constitucional del secreto de las comunicaciones. En Revista Española de Derecho Constitucional, nº 20, pp. 42 y ss.

Martínez Martínez, R. (2004). Una aproximación crítica a la autodeterminación informativa. Madrid: Thomson-Civitas.

Narváez Rodríguez, A. (1999). Intervenciones telefónicas. En Repertorio Aranzadi del Tribunal Constitucional, vol II, Pamplona: Aranzadi.

Pulido Quecedo, M. (2006). La noción de «secreto de las comunicaciones postales» ex art. 18.3 CE. En Repertorio Aranzadi del Tribunal Constitucional, núm. 16/2006, Pamplona: Aranzadi.

Vilasau, M. (2006). La Directiva 2006/24/CE sobre conservación de datos de tráfico en las comunicaciones electrónicas: seguridad v. privacidad. IDP. En Revista de Internet, Derecho y Política, nº 3, UOC. Recuperado fecha de consulta 10/05/2007, en http://www.uoc.edu/ojs/index.php/idp/article/view/398.

Retos y oportunidades del entretenimiento en línea.
Actas del *VIII Congreso Internacional Internet, Derecho y Política (IDP 2012)*

ISBN: 978-84-695-4123-4

Para citar la obra, por favor, utilicen las
siguientes referencias indistintamente:

Cerrillo i Martínez, A., Peguera, M., Peña-López, I., Pifarré de Moner, M.J.,
& Vilasau Solana, M. (coords.) (2012). *Retos y oportunidades del entretenimiento en línea*.
Actas del VIII Congreso Internacional, Internet, Derecho y Política. Universitat Oberta
de Catalunya, Barcelona 9-10 Julio, 2012. Barcelona: UOC-Huygens Editorial.

Cerrillo i Martínez, A., Peguera, M., Peña-López, I., Pifarré de Moner, M.J., & Vilasau Solana,
M. (coords.) (2012). *Challenges and Opportunities of Online Entertainment*. Proceedings of
the 8th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya,
Barcelona 9-10 July, 2012. Barcelona: UOC-Huygens Editorial.

http://edcp.uoc.edu/symposia/idp2012/proceedings/

UOC
Universitat Oberta de Catalunya
www.uoc.edu

HUYGENS
EDITORIAL